orange™ Business Services

Secure Authentication

end-user guide

version 1.1

Publication History

Date	Description	Revision
2013.04.05	initial release (concatenation of separate end-user guides)	1.0
2013.07.25	Enrollment process description updated	1.1

welcome

Orange Business Services would like to thank you for choosing our Secure Authentication service to help you protect your on-line identity and the networks, applications and data you use from unauthorized access.

This guide is intended for people in your company:

- that will use our Secure Authentication service (end-users).
- that will manage our Secure Authentication service (administrators).

This guide includes troubleshooting tips (marked with a yellow flag):
If these tips fail, contact your usual help desk to arrange for a troubleshooting session.

Click on the picture related to the token you want to use to directly access the right documentation part.

<table>
<tr><th colspan="3">MP software token</th></tr>
<tr><td>MP for Windows PC
  </td><td>MP for OSX Lion
  </td><td>MP for Apple iOS
  </td></tr>
<tr><th colspan="3">KT hardware token</th></tr>
<tr><td colspan="2">KT-5 token
  </td><td>KT-4 token
  </td></tr>
<tr><th colspan="3">Grid token</th></tr>
<tr><td colspan="3">GrIDsure
  </td></tr>
<tr><th colspan="3">Password</th></tr>
<tr><td colspan="3">Password
  </td></tr>
</table>

Contents

Figures

Secure Authentication End User Rules

These Rules of Use apply to your use of the enclosed token, card or other device (your Device) and your secret Personal Identification Number (your PIN).

You should use your Device and your PIN to identify yourself to any systems or service secured the Orange Secure Authentication service in accordance with these Rules and any written agreements between yourself and your organization and your organization and Orange.

It is important that you take proper care of your Device, keep it safe and secure at all times and guard against loss, damage and theft.

Your PIN must remain secret to you at all times. **No other person ever needs to know this PIN and you should not disclose it to anyone**. This includes your colleagues and systems administrators at your company and personnel who are, or claim to be representatives of Orange or a Partner of Orange. You should be extremely suspicious of anyone who ever tells you at they need to know your PIN, and you should report any such incident to your Administrator immediately.

The privacy of your Device and the confidentiality of your PIN are crucial to the verification of your on-line identity and the security of your information and the networked system(s) that may be accessed using your identity.

If your Device is lost, damaged or stolen, or if you believe that the confidentiality of your secret PIN has been compromised in any way, you should report these incidents immediately to your Administrator. Upon receiving the notice, the Administrator will then disable your Device or allow you to change your PIN, to ensure that no third party may misuse them.

If you do not report these incidents immediately, there is the risk that someone else may steal your on-line identity. Any activities they carry out using your identity will compromise the security and integrity of your information and systems. You may be held legally responsible for activities that are perpetrated using your identity.

You must not give away, sell, rent or lend your Device even to someone you believe to be an authorized user of the system.

You must not mistreat damage or open your Device or try to reverse-engineer, decompile, disassemble, translate, copy, and alter the Device (or any of its components).

If you lose or break your Device a replacement fee will be charged by Orange to your organization.

Should your account be terminated, for any reason, or if you have no further need to use the system, you must contact your Administrator immediately to disable your Device and then follow instructions from your Administrator to have it safely returned.

MP token for Windows PC

In this chapter, you will find instructions for installing, activating and managing your MP token for Windows PC devices.

The advantage of software tokens is mass deployment without hardware distribution. By thoughtful selection of the type of device upon which a software token can be installed, administrators can lock an end-user to a specific machine, limit the end-user to using only secure platforms or provide complete machine independence.

With our Secure Authentication service, MP tokens can be issued, revoked and reissued without restriction or the need to recover the MP token from the end-user. Multiple MP software tokens can be installed on a single device (e.g. hard drive) provided the usernames are unique.

what is a MP token?

Up until now, you've logged on with your User Name and Password. The problem is that passwords are easily compromised, putting your identity and the resources you access at risk. By using a MP token, you will be able to generate a "One-time Password" or "OTP". As the name implies, an OTP can only be used once. Each time you logon you will use your MP to generate a new OTP.

how does it protect me?

Password theft is the single most common way thieves and hackers steal identities and gain unauthorized access to networks and resources. While they have many ways to steal a password, success depends on the stolen password being valid, much the way credit card theft relies on the card being usable until you report it as stolen. The problem of course is that it is almost impossible for you or the security professionals that manage your network to discover your password has been compromised until long after damage has been done.

The MP token solves this problem because the instant you logon with your OTP, it is no longer valid. Any attempt to logon by reusing the OTP will not only fail, but also instantly alert your network security professionals to a possible attack on your identity.

can anybody use my MP token?

Thanks to PIN Code protection, your MP token is protected against unauthorized use by a PIN Code only you know. Again, much like a bank card or "Chip and PIN" credit card, the thief not only needs access to your MP token but must know your PIN Code as well. Any attempt to use the MP token with and incorrect PIN Code will fail. Successive attempts to guess your PIN Code will automatically "lock" your MP token, effectively disabling it, giving you and your network security professionals time to deal with the threat.

what kind of PIN Code is supported by MP token?

- **Server-side user-selected PIN Code:** the PIN Code is stored and managed at the Secure Authentication server level. You have the ability to change it at any time. Token Codes are generated without entering any PIN Code in the "Token" application (OTP=PIN Code+Token Code).
- **Server-side fixed PIN Code:** the PIN Code is stored and managed at the Secure Authentication server level. The PIN Code displayed during MP token installation is permanent, you can not change it. Token Codes are generated without entering any PIN Code in the "Token" application (OTP=PIN Code+Token Code).
- **Client-side user-selected PIN Code:** the PIN Code is stored and managed at the Windows PC level. You have the ability to change it at any time. The PIN Code must be entered into the "Token" application to generate a Token Code (OTP=Token Code).
- **Client-side fixed PIN Code:** the PIN Code is stored and managed at the Windows PC level. The PIN Code displayed during MP token installation is permanent, you can not change it. The PIN Code must be entered into the "Token" application to generate a Token Code (OTP = Token Code).

what are Software Tools?

Software Tools is a set of applications you have to install on your Windows PC to install, activate and manage your MP tokens. “Token” and “Token Manager” applications are part of these Software Tools.

what is the “Token” application?

The “Token” application allows you to:

- select a MP token when several are installed
- generate a Token Code from a MP token
- rename a MP token
- resynchronize a MP token
- change the PIN Code of a MP token (when client-side PIN Code type is used)
- unlock a MP token when the feature is allowed by your Secure Authentication service administrators.
- retrieve the version of the “Token” application

what is “Token Manager” application?

The “Token Manager” application allows you to:

- select a MP token when several are installed
- retrieve the serial number of a MP token
- remove a MP token from your Windows PC

what are my responsibilities?

Using the MP token will not only provides security, it will simplify your life be reducing or eliminating the need to remember or periodically change passwords. Your MP token will do this for you, every time you logon. However, you do have a few simple obligations.

protect your PIN Code

You have to protect your PIN Code just as you would the PIN Code for your bank or credit card. Never share it with anybody, including people you trust. Your usual help desk will never ask for your PIN Code and you should never reveal it to them. Never write down your PIN Code.

what if I forget my PIN Code?

Contact your usual help desk. Upon verifying your identity they will be able to reset your PIN Code.

what if my MP token is locked?

Contact your usual help desk. Upon verifying your identity they will be able to unlock your MP token.

how long will my MP token continue to operate?

Your MP token will be able to generate OTPs until it is revoked by IT administrators.

what should I do if I can't logon using my token?

The most common cause of failed logon is entering an incorrect OTP. Never attempt to reuse a Token Code and ensure that you enter the Token Code exactly as displayed on the token, including any upper and lower case letters and punctuation that it may contain.

By default, your account will automatically lock for 15 minutes if more than 3 consecutive logon attempts fail. You must wait this amount of time before your account will unlock. Contact your usual help desk to resolve logon problems.

how do I enroll with a MP token?

When using Internet Explorer as Web browser

From the Internet Explorer menu bar, select "Tools", "Internet Options", "Security" tab, "Trusted sites" zone, click on "Sites", and add the following URL:

https://se.safenet-inc.com

This setting will allow your Internet Explorer web browser to install and run the Software Tools activeX control.

how do I access the enrollment web site?

Within your e-mail client: open the "SAS Self-enrollment" message 1, and click on the self-enrollment URL link 2: your web browser will connect to the Secure Authentication enrollment web site.

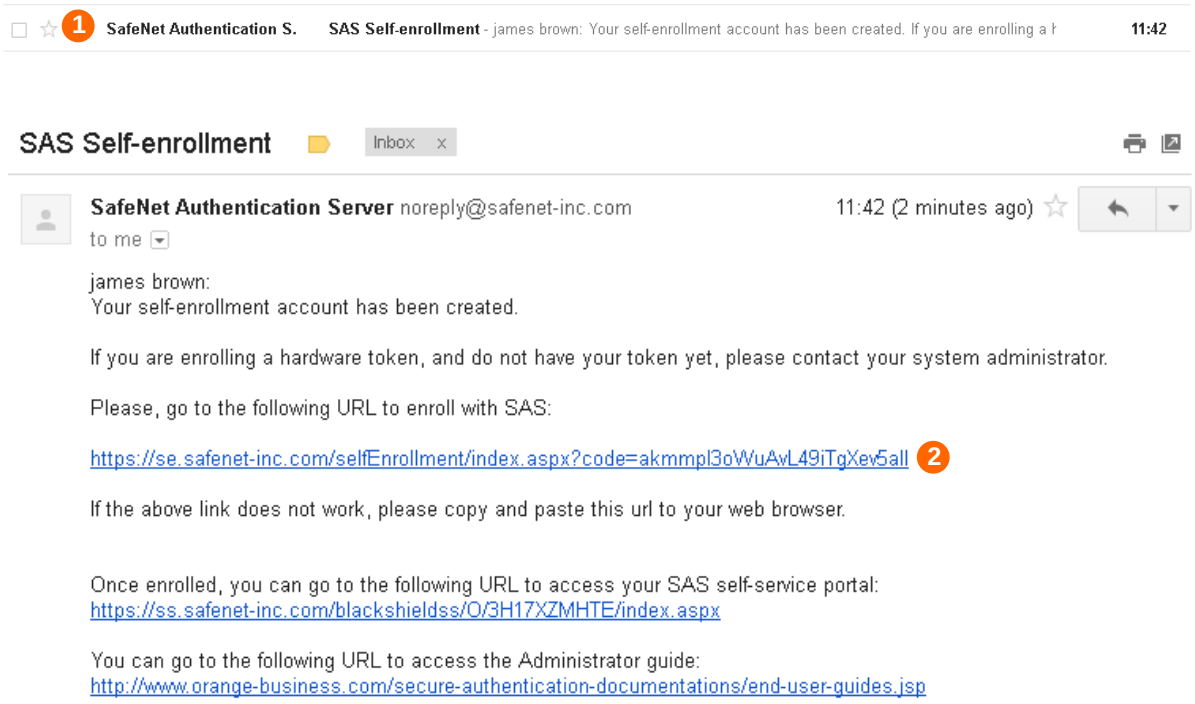

Figure 1: self-enrollment link

- **"SAS Self-enrollment" e-mail not received:** verify if the mail is not stored in the "junk" folder of your e-mail client.
- **"Your provisioning task has already been completed" error message:** verify you opened the latest self-enrollment message, and not an old one.

how do I select a Windows PC as target device?

Within your web browser: select “Install Locally” ❶, then click on “Next” ❷.

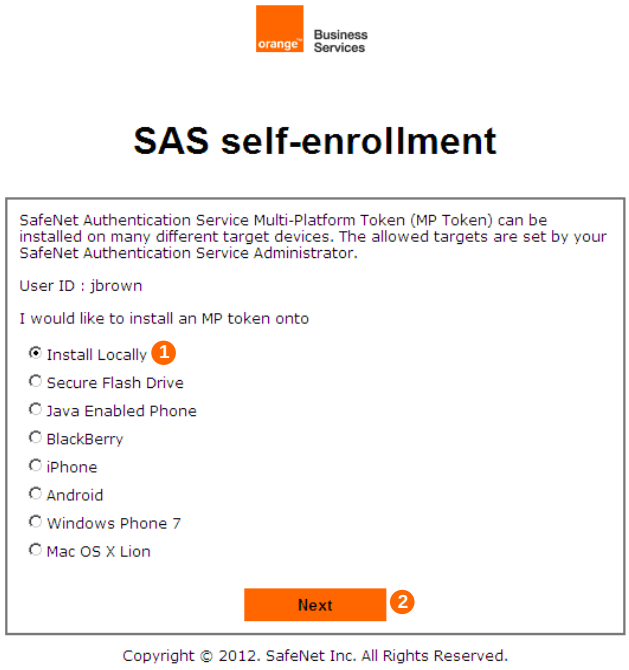

Figure 2: select Windows PC as target device

how do I download the Software Tools installer?

Within your web browser: click on “Download Software Tools and Activatye Token” link ❶ (that automatically points to the adapted 32-bit or 64-bit Software Tools installer), then click on “Next” ❷.

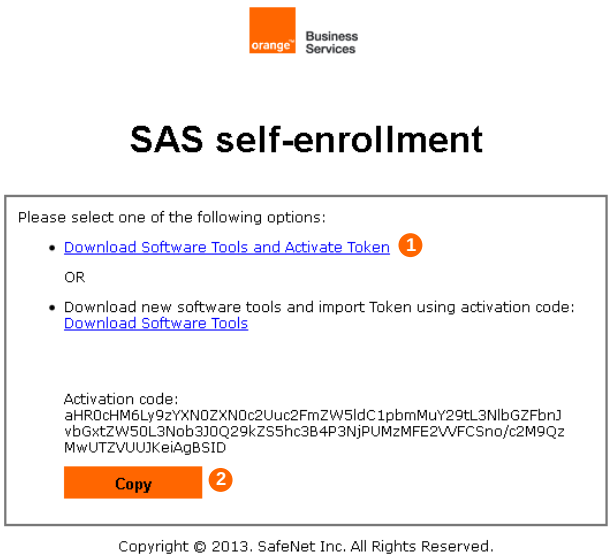

Figure 3: download Software Tools installer

how do I run the Software Tools installer

You must have **administrator rights** on your Window PC to run the Software Tools installer.

Internet Explorer

Within the Software Tools installer: click on "Run" ❶ (if a "Security Warning" pop-up window is displayed, click on "Run" ❷ to accept the publisher of the installer).

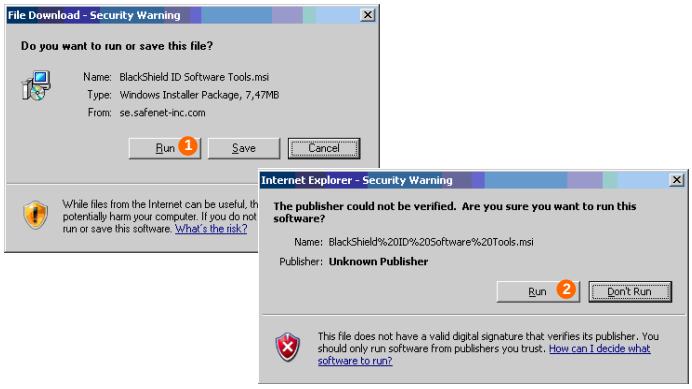

Figure 4: run Software Tools installer (within Internet Explorer)

Firefox

If your Firefox browser displays **Additional plugins are required to display all the media on the page** banner, close it.

Within the Software Tools installer: click on "Save File" ❶, save the Software Tools installer file locally ❷, then click on the file name ❸ to run the installer.

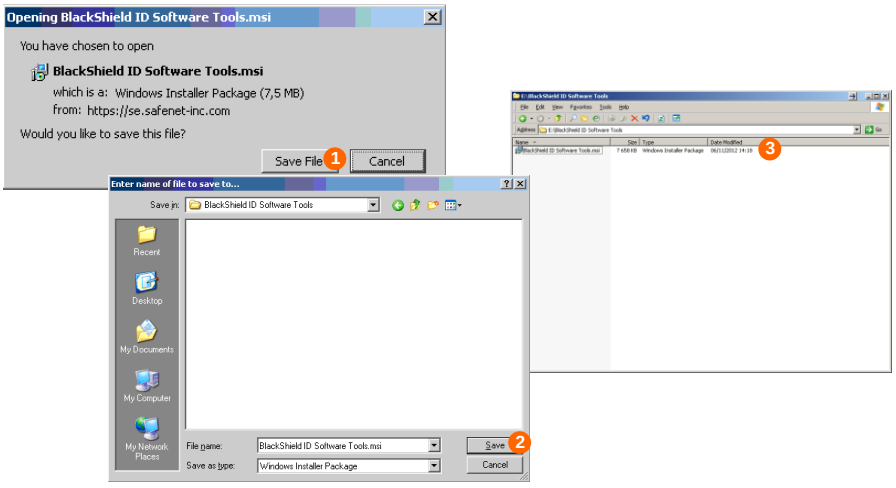

Figure 5: run Software Tools installer (within Firefox)

how do I install the Software Tools?

Within the Software Tools installer: click on “Next” ❶, accept the terms in the license agreement ❷, click on “Next” ❸, enter your user name and your organization name ❹, install the application for “anyone who uses the computer (all users)” ❺, click on “Next” two times ❻❼ (do not change the install directory), click on “Install” ❽, then on “Finish” ❾ at the end of the Software Tools installation.

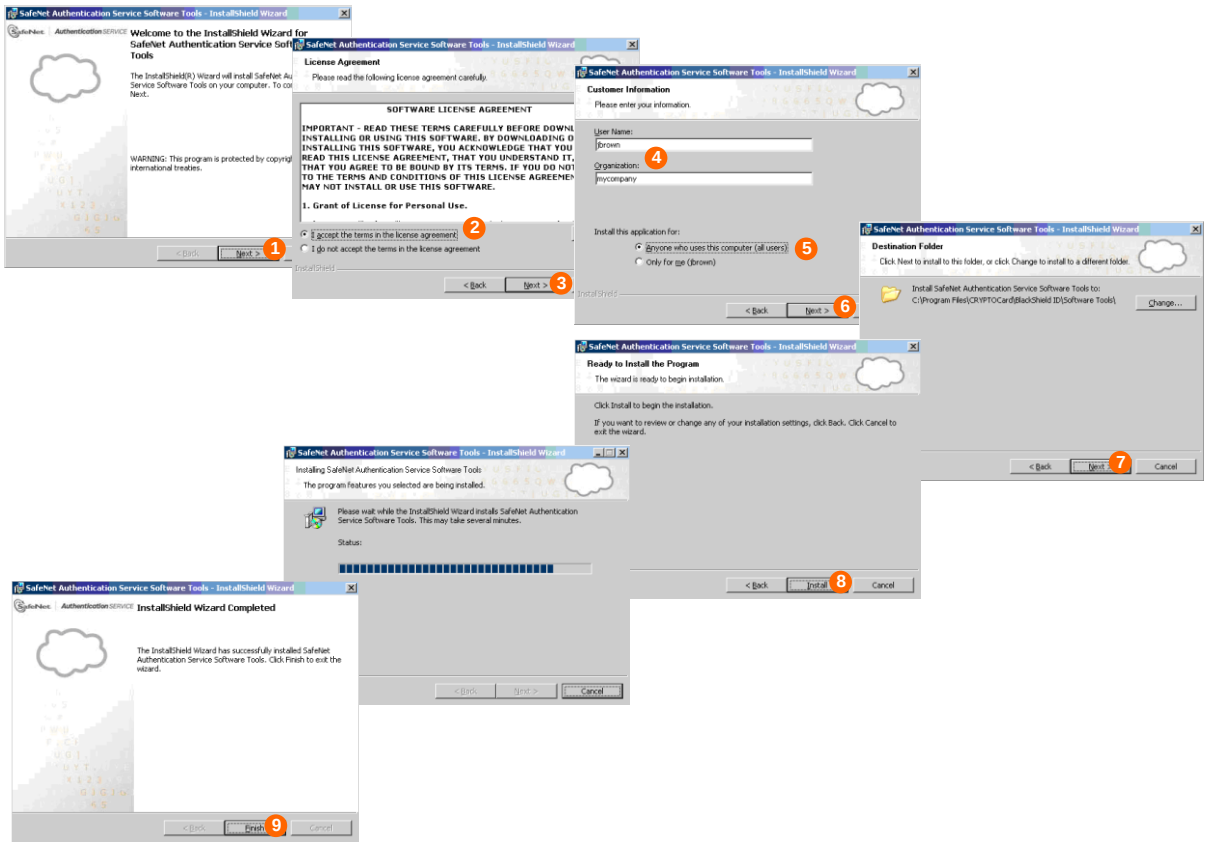

Figure 6: install Software Tools

how do I download the MP token file?

Internet Explorer

The MP token file download step is automatically managed by the Software Tools ActiveX.

- **"Token file download" page remains displayed on your Internet Explorer browser:** verify the Software Tools ActiveX control is enabled: upon your browser select "Tools", "Manage Add-ons", "Enable or Disable Add-ons…", "Add-ons that have been used by Internet Explorer" in the "Show" drop-down list. The ActiveX control named "activeXWebAPIControl" must be referenced. Verify you defined the SafeNet URL as trusted site (see ***Error! Reference source not found.*** chapter).

Firefox

If your Firefox browser displays **Additional plugins are required to display all the media on the page** banner, close it.

Click on "Download" ❶, open the token file with BlackShield Token application ❷, click on "Next" ❸, enter the PIN displayed on the web page (here 0000) into the PIN "field" of the MP application ❹, if needed select the MP token you want to use and click on "Generate Token Code" ❺, enter the PIN displayed on the web page (here 0000) followed by the new generated Token Code ❻, then click on "Next" ❼.

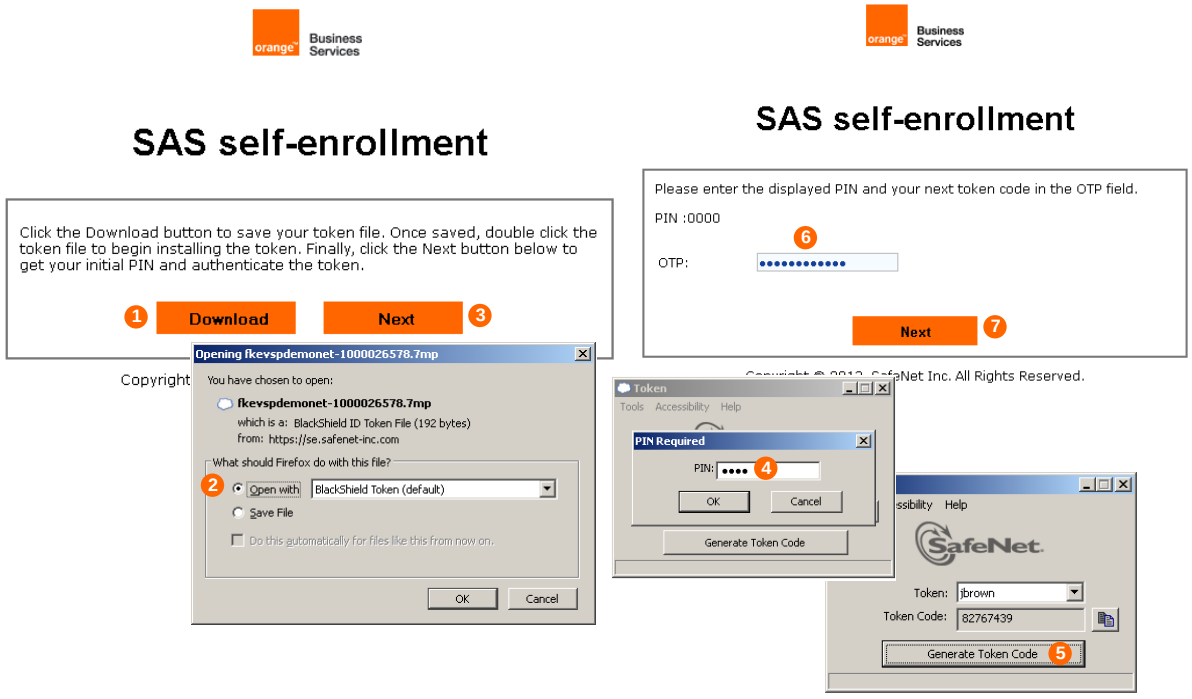

Figure 7: download token file

how do I install the MP token file with fixed PIN?

Within your web browser: memorize the displayed PIN Code ❶ (this will be your definitive PIN Code), then click on "OK" ❷. The enrollment web site displays a page that confirms your MP token has been successfully activated. Memorize your User ID ❸, then click on "Close" ❹ (when using Firefox, you have to close the browser).

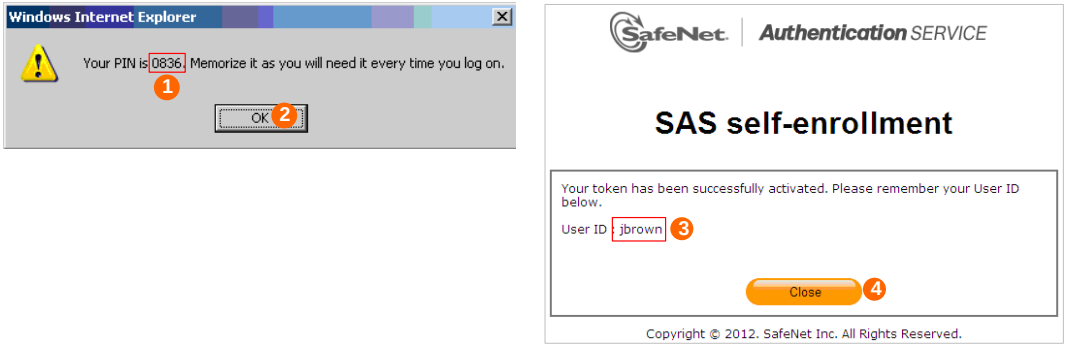

Figure 8: install token file (with fixed PIN Code)

how do I install the MP token file with user-selected PIN?

Within your web browser: choose your PIN Code, enter it in the "New PIN" and "Verify PIN" fields ❶ then click on "Next" ❷. The enrollment web site displays a page that confirms your MP token has been successfully activated. Memorize your User ID ❸, then click on "Close" ❹ (when using Firefox you have to close the browser).

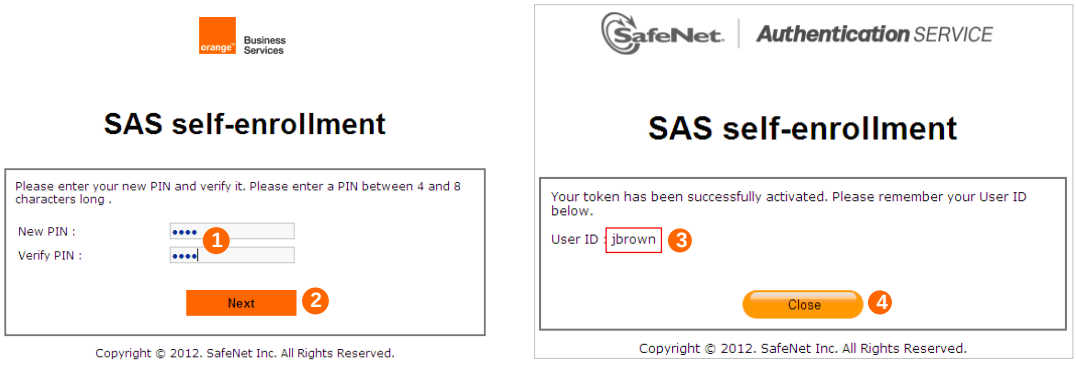

Figure 9: install token file (with user-selected PIN Code)

- **"PIN change failed" error message:** try to enter your new PIN Code again making sure to meet complexity requirements displayed.
- **"You have failed to provide the correct response too many times" error message:** contact your usual help desk.

how do I launch the “Token” application?

Within the Windows taskbar: click on “Start”, “Programs”, “SafeNet”, “Tokens” two times“.

how do I select my MP token?

Within your “Token” application: when only one MP token is installed, it is automatically selected ❶, else use the dropdown menu ❷ to select the MP token you want to use.

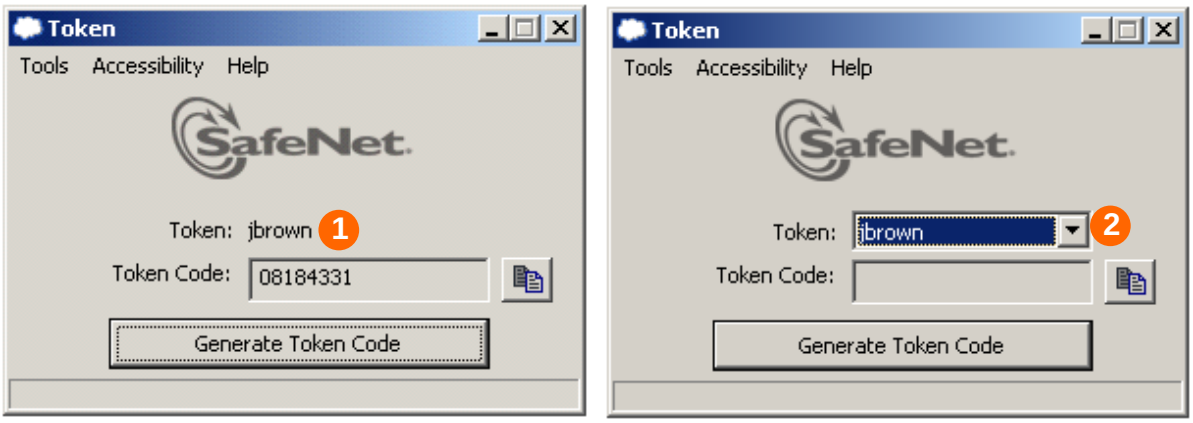

Figure 10: select token

how do I authenticate with my MP token?

You have the ability to test authentication with your MP token thanks to the SAS self-service portal.

1. **Within your e-mail client:** open the “SAS Self-enrollment” message 1 again, and click on the SAS self-service portal URL link 2: your web browser will connect to the self-service web site.

2. **Within the SAS self-service portal:** within the “Home” page click on “Sign In” 3, within the “Authenticate” page click on “Sign in using your token” 4.

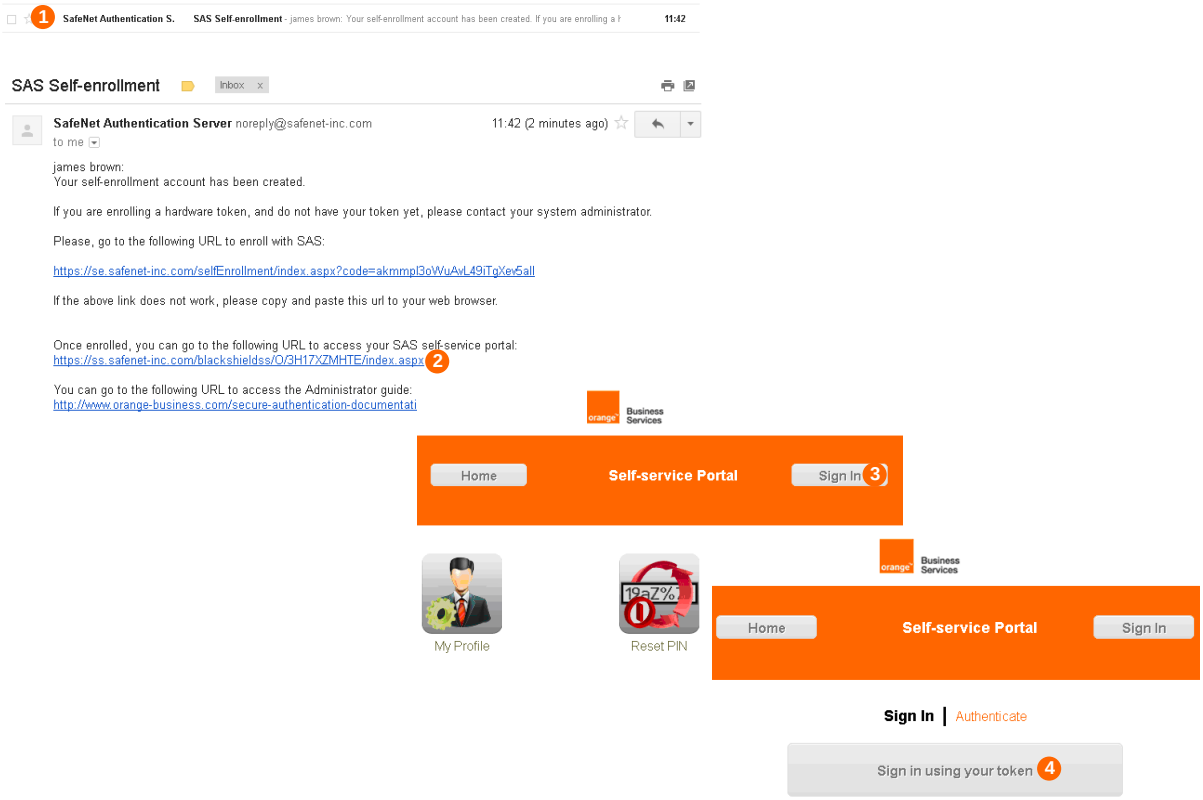

Figure 11: access to the SAS self-service portal sign in page

The authentication process depends on the type of the MP Token PIN Code

server-side PIN Code

1. **Within the SAS self-service portal:** within the "Authenticate to Process" page enter your user ID in the "User ID" field ❶ and your PIN Code in the "OTP" field ❷.
2. **Within your "Token" application:** click on "Generate Token Code" ❸, then on "Copy" ❹.
3. **Within the SAS self-service portal:** within the "Authenticate to Process" page paste the Token Code value next to the PIN Code in the "OTP" field ❺, then click on "OK" ❻. The "Sign Out" button ❼ displayed within the "Home" page indicates your authentication is successful.

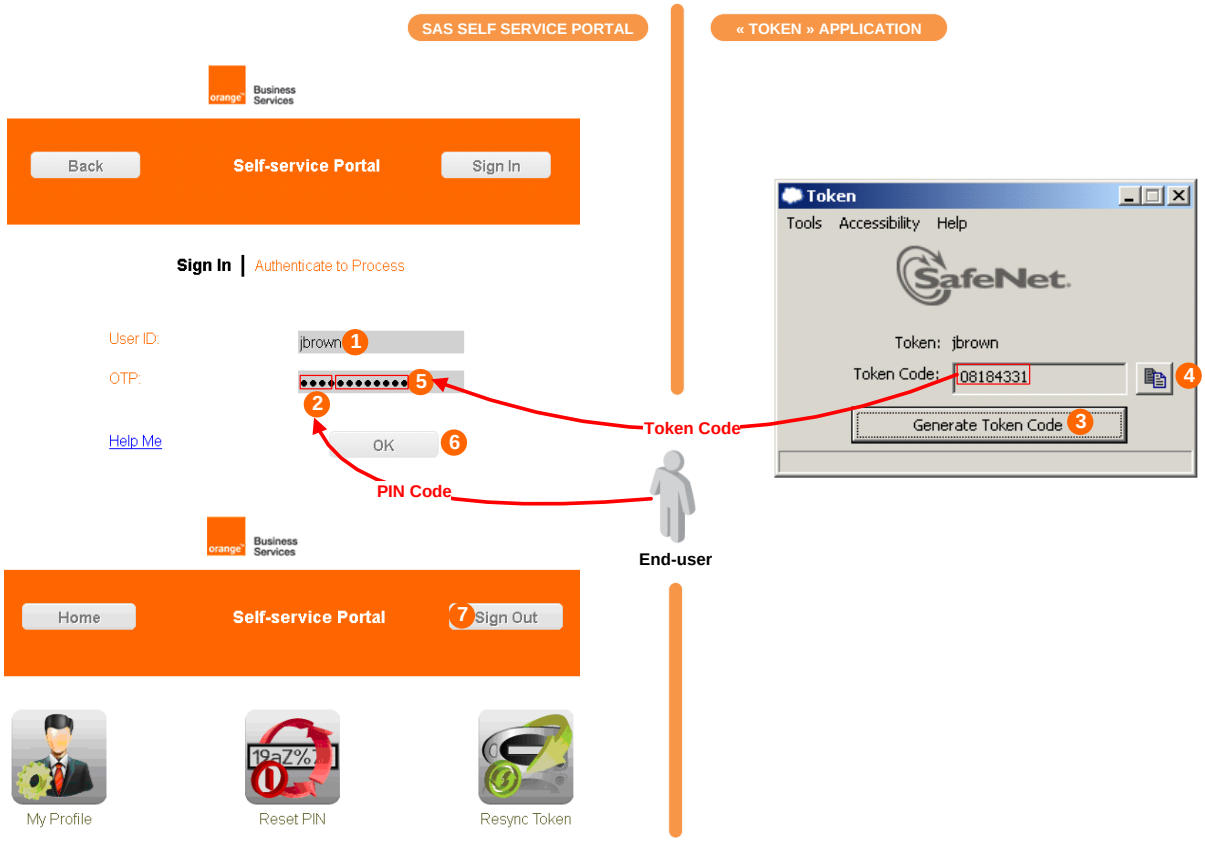

Figure 12: authenticate (with server-side PIN Code)

- **"Your login attempt was not successful" error message:** try to authenticate again, making sure to enter your PIN Code followed by the Token Code generated by your MP token in the "OTP" field.

client-side PIN Code

1. **Within the SAS self-service portal:** within the "Authenticate to Process" page enter your user ID in the "User ID" field 1.

2. **Within your "Token" application:** click on "Generate Token Code" 2, within the pop-up windows enter your PIN Code in the "PIN" field 3, click on "OK" 4, then on "Copy" 5.

3. **Within the SAS self-service portal:** within the "Authenticate to Process" page paste the Token Code value in the "OTP" field 6, then click on "OK" 7. The "Sign Out" button 8 displayed within the "Home" page indicates your authentication is successful.

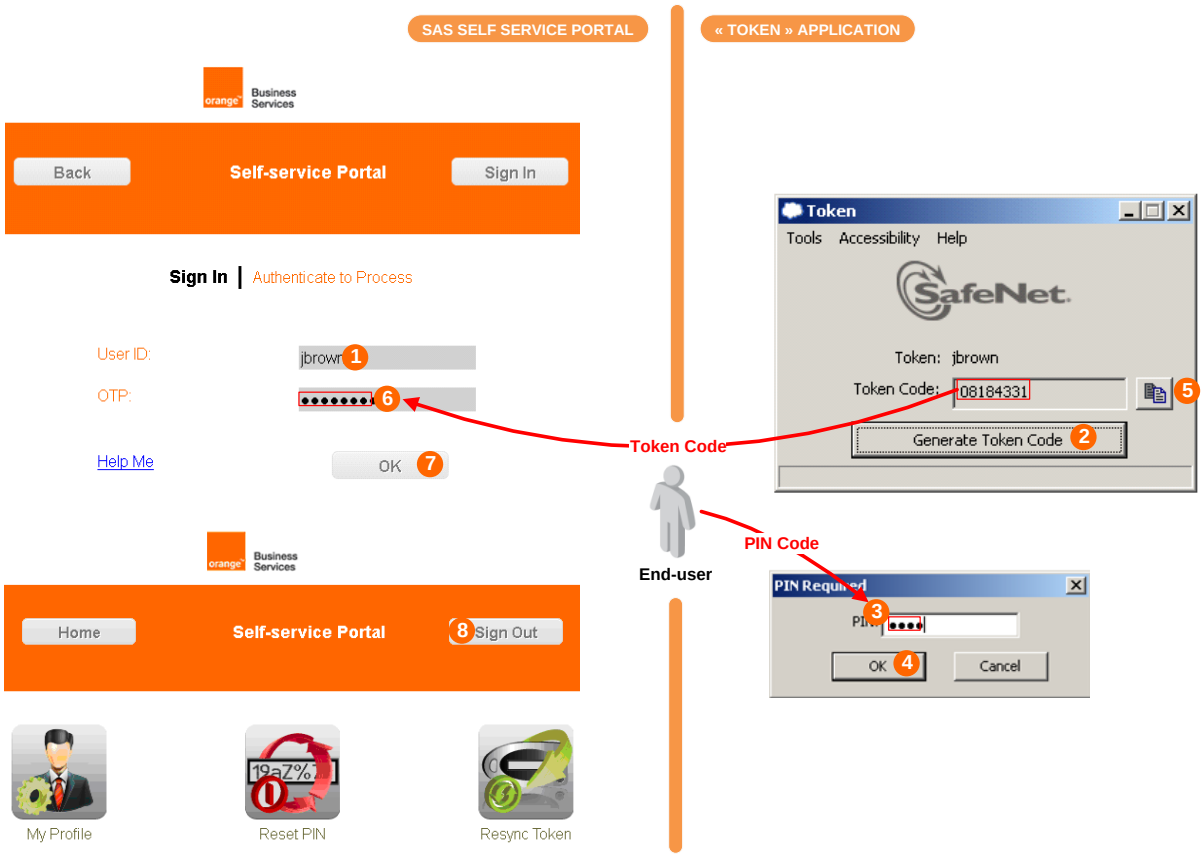

Figure 13: authenticate (with client-side PIN Code)

- **"Your login attempt was not successful" error message:** try to authenticate again, making sure to enter only the Token Code generated by your MP token in the "OTP" field.

how do I change my PIN Code?

The PIN Code change process depends on the type of the MP Token PIN Code.

server-side PIN Code

Within the SAS self-service portal: within the "Home" page, once authenticated ("Sign Out" button must be displayed 1), click on "Reset PIN" 2, within the "Create New PIN" page choose a new PIN Code and enter it in the "Create New PIN" and "Verify PIN" fields 3, then click on "OK" 4. Within the "Create New PIN" page a message indicates your PIN Code change is successful 5.

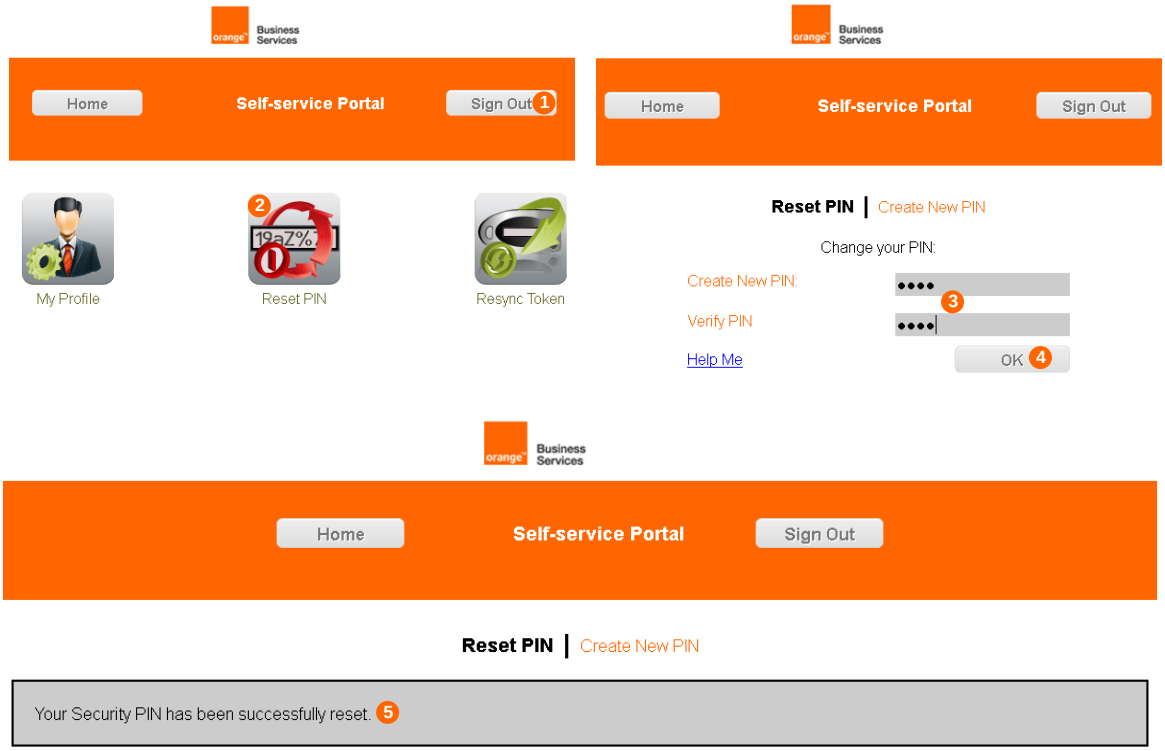

Figure 14: change server-side PIN Code

- **"No tokens are enabled to change the Personal Identification Number (PIN)" error message:** your MP token has not a server-side PIN Code but a client-side instead.

client-side PIN Code

Within your "Token" application: select "Tools", "Change PIN" 1, enter your current PIN Code in the "Current PIN" field 2, choose a new PIN Code and enter it in the "New PIN" and "Verify New PIN" fields 3, then click on "OK" 4. At the bottom of your "Token application" a message indicates your PIN Code change is successful. 5.

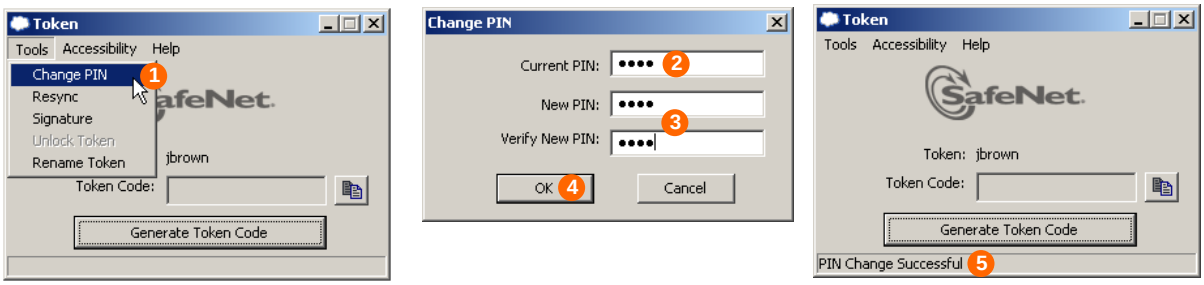

Figure 15: change client-side PIN Code

- **"PIN Change Failed" error message:** try to change your PIN Code again, making sure to enter a complex one, the correct number of characters, and the correct types **of character.**

how do I resynchronize my MP token?

Within the SAS self-service portal: within the "Home" page click on "Resync Token" 1, within the "User" page enter your user ID in the "User ID" field 2, click on "Next" 3 , enter the serial of your MP token in the "Serial" field 4, then click on "Next" 5.

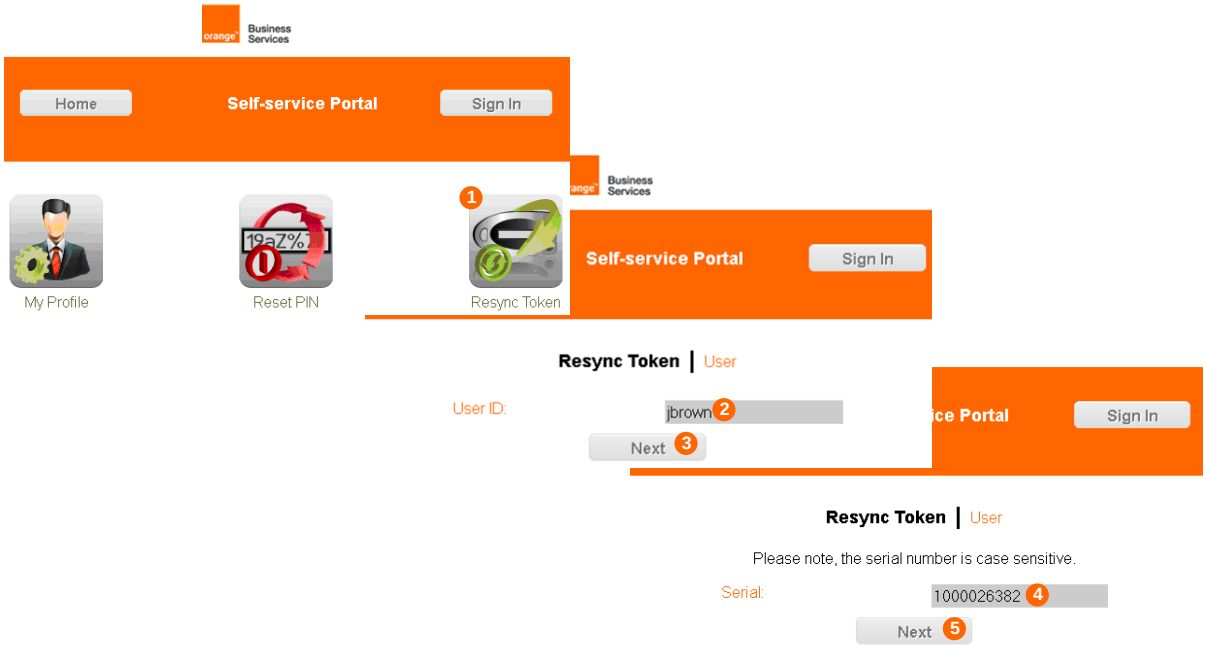

Figure 16: resynchronize token (common part)

The end of the resynchronization process depends on the type of the MP Token PIN Code.

server-side PIN Code

1. **Within the SAS self-service portal:** within the "Challenge/Response" page copy the "Respond to challenge" value ❶.

2. **Within your "Token" application:** select "Tools", "Resync" ❷, within the pop-up window paste the challenge value in the "Challenge" field ❸, click on "OK" ❹, then click on "Copy" ❺ to copy the generated response.

3. **Within the SAS self-service portal:** within the "Challenge/Response" page paste the response value in the "Response" field ❻, then click on "OK" ❼. Within the "Confirmation" page a message indicates your token resynchronization is successful ❽.

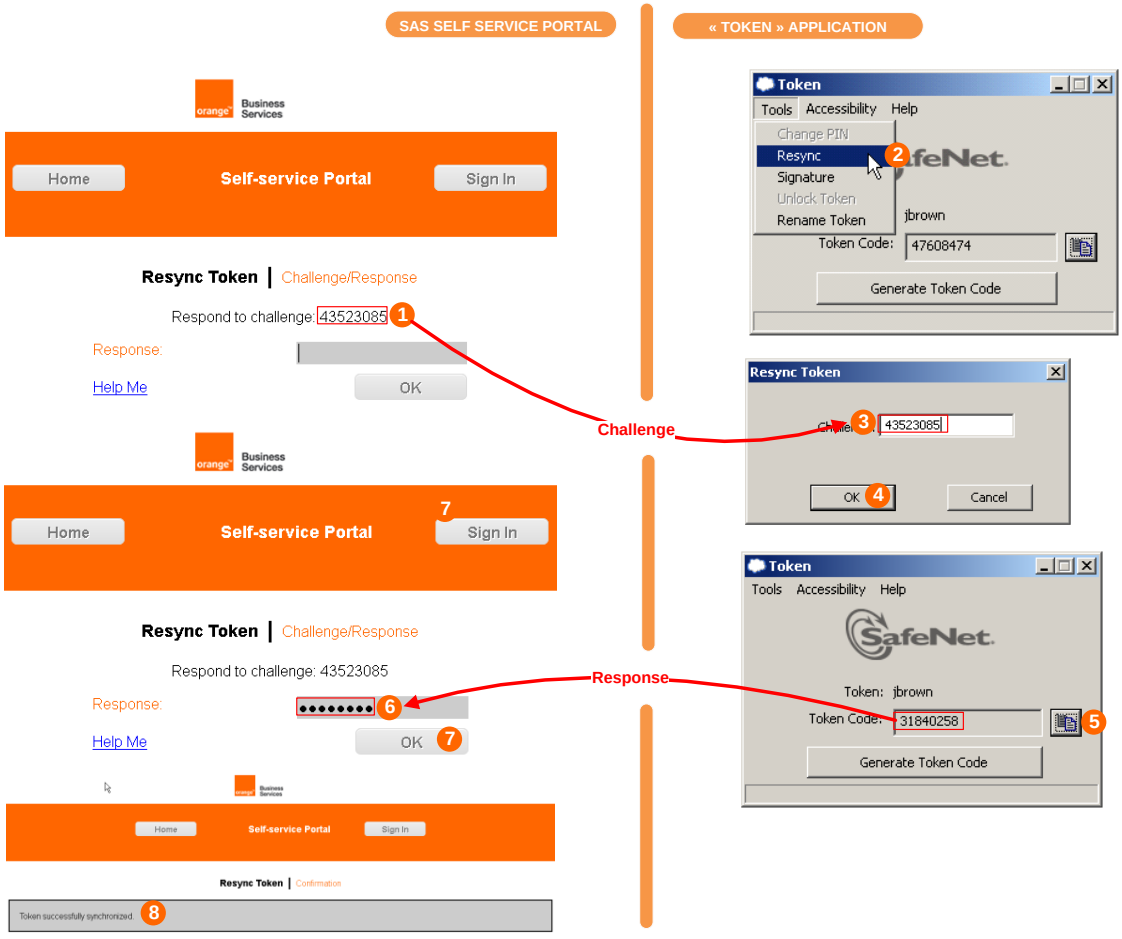

Figure 17: resynchronize token (with server-side PIN Code)

- **"The token cannot be synchronized" error message:** try to resynchronize your MP token again, making sure to copy/paste the right challenge/response values.

client-side PIN Code

1. **Within the SAS self-service portal:** within the "Challenge/Response" page copy the "Respond to challenge" value 1.

2. **Within your "Token" application:** select "Tools", then "Resync" 2. Within the pop-up window paste the challenge value in the "Challenge" field 3, enter your PIN Code value in the "PIN" field 4, click on "OK" 5, and then click on "Copy" 6 to copy the generated response.

3. **Within the SAS self-service portal:** within the "Challenge/Response" page paste the response value in the "Response" field 7, then click on "OK" 8. Within the "Confirmation" page a message indicates your token resynchronization is successful 9.

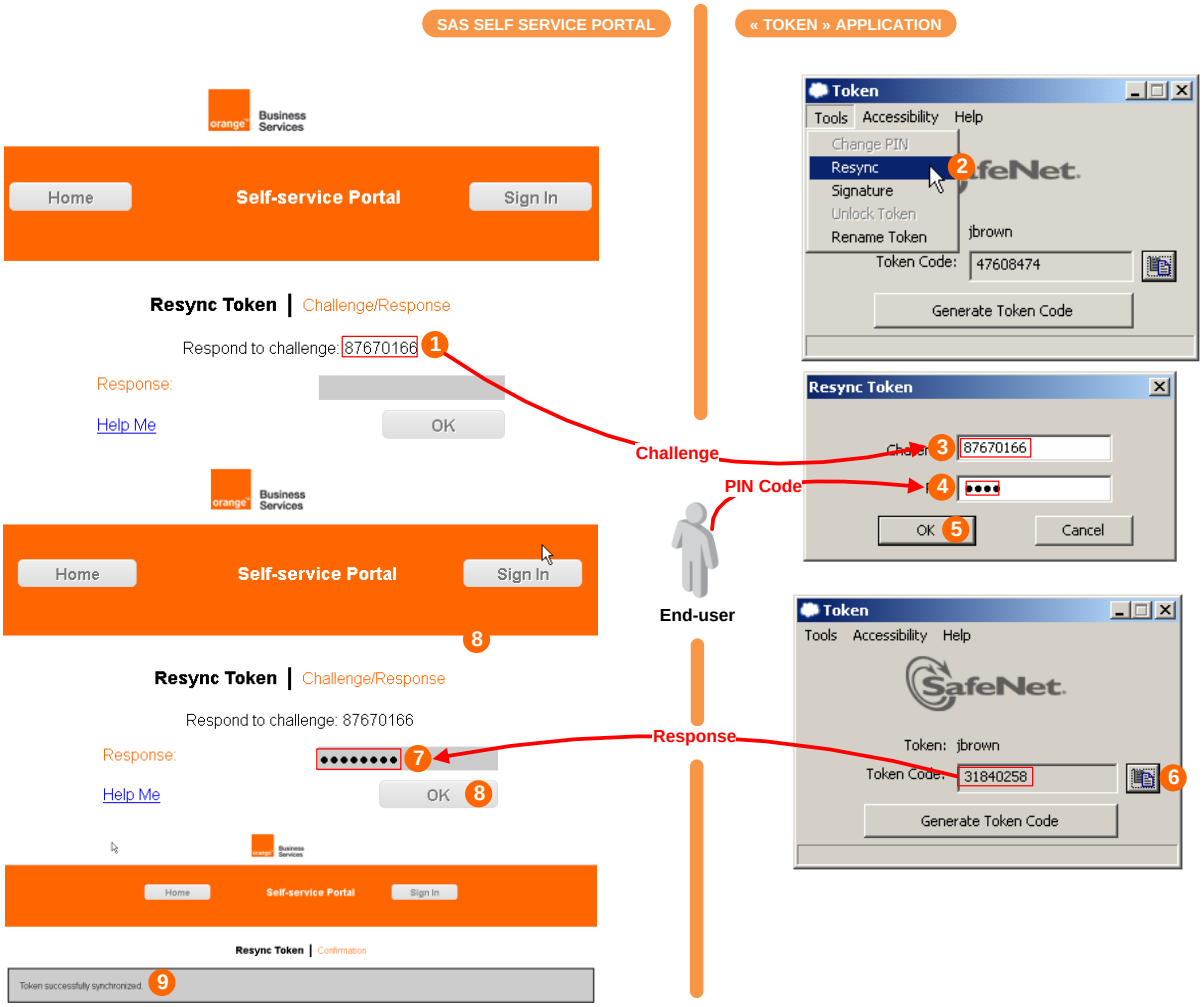

Figure 18: resynchronize token (with client-side PIN Code)

- **"The token cannot be synchronized" error message:** try to resynchronize your MP token again, making sure to copy/paste the right challenge/response values.

how do I rename my MP token?

By default, MP token name is based on your user ID.

Within your "Token" application: select "Tools", "Rename Token" ❶, within the pop-up window enter the new MP token name in the "New Name" field ❷, then click on "OK" ❸. Your MP token is now referenced with the new name ❹.

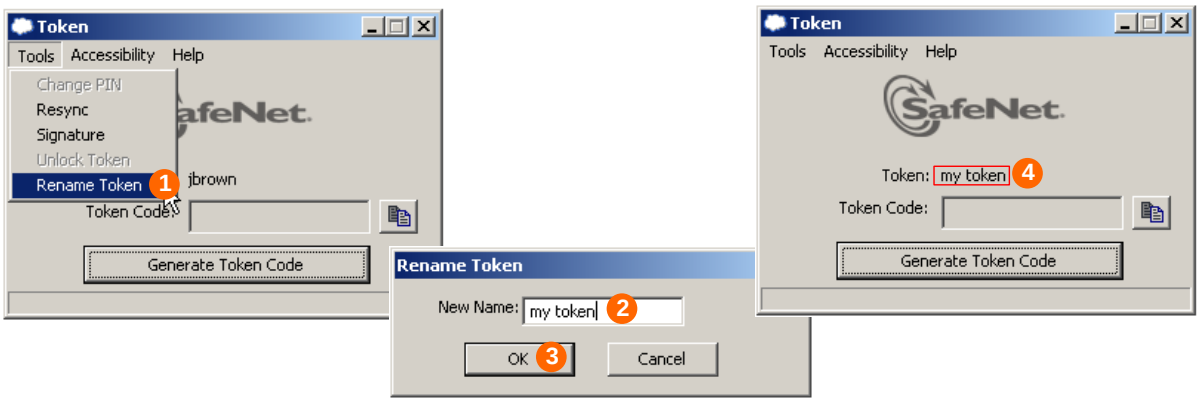

Figure 19: rename token

how do I retrieve the "Token" application version?

For maintenance or troubleshooting purposes, your IT administrator may ask you the version of your Token application MP.

Within your "Token" application: select "Help", "About" ❶, memorize the "Token" application version ❷, then click on "OK" ❸.

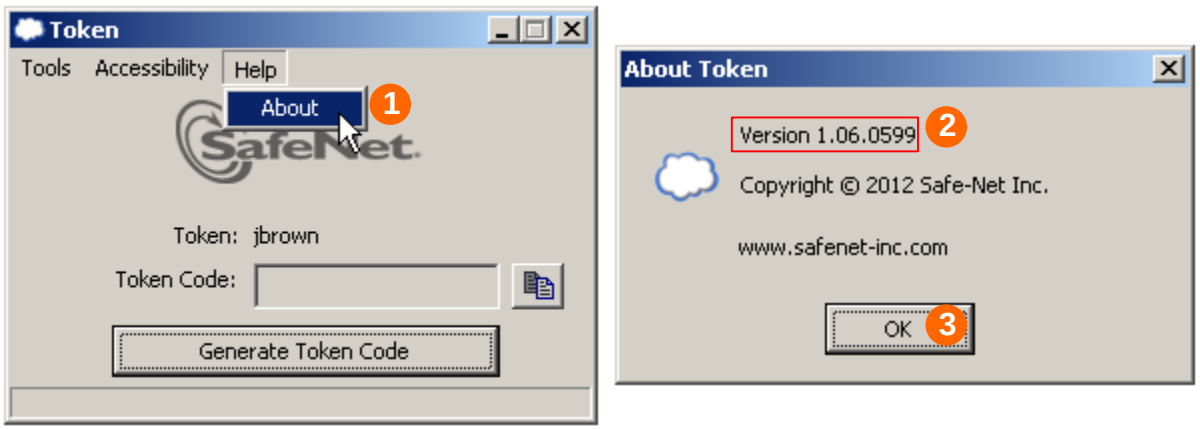

Figure 20: retrieve "Token" application version

how do I launch the “Token Manager” application?

- **Windows XP:** within the Windows taskbar, select “Start”, “Settings”, “Control Panel”, “BlackShield ID Token Manager”.
- **Windows 7:** within the Windows taskbar, select “Start”, “Control Panel”, “BlackShield ID Token Manager”.

how do I retrieve my MP token serial?

Within your “Token Manager” application: select the token you want to find the serial ❶, click on “Token Information” ❷, within the pop-up window memorize the MP token serial ❸, then click on “Close” ❹.

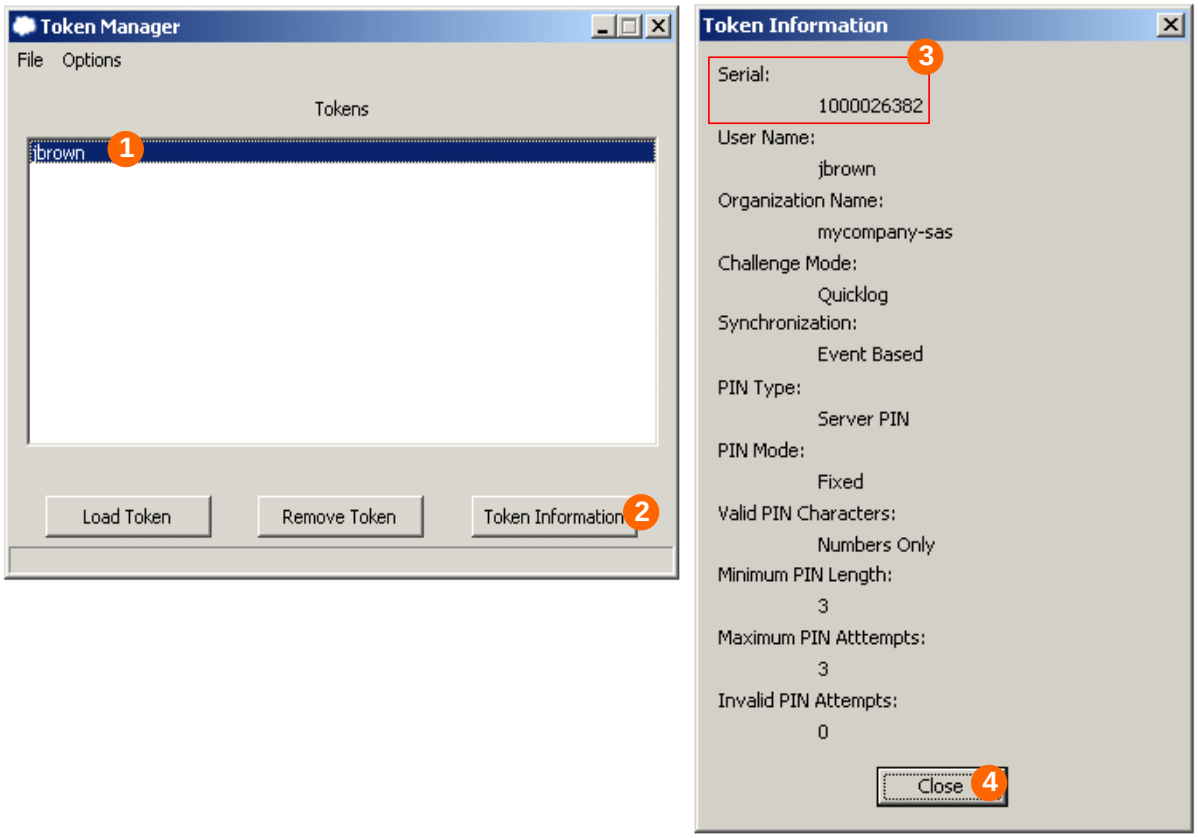

Figure 21: retrieve token serial

how do I remove my MP token?

For maintenance or troubleshooting purposes, your IT administrator may ask you to remove a MP token from your device.

Within your "Token Manager" application: select the token you want to remove 1, click on "Remove Token" 2, within the pop-up window click on "Yes" 3.The token has been successfully removed 4.

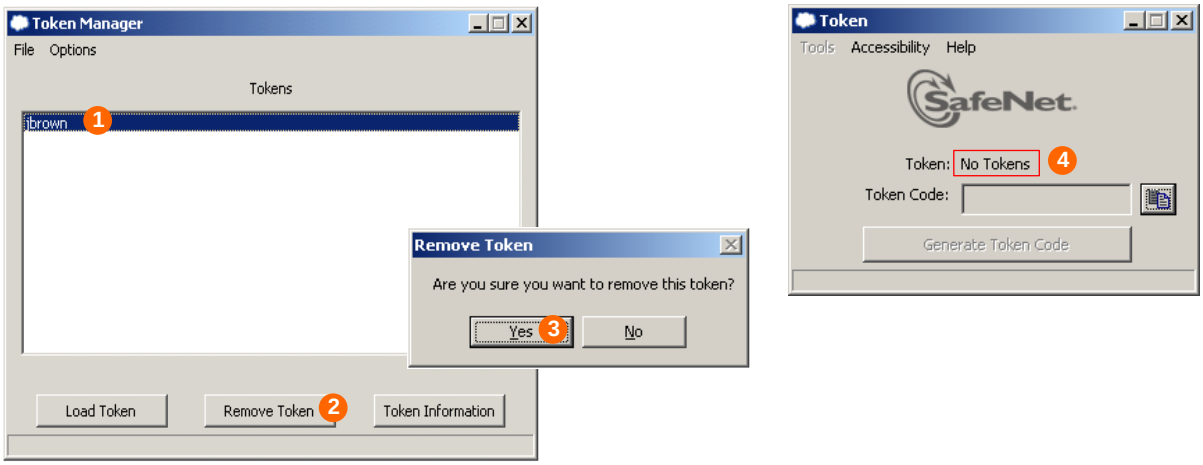

Figure 22: remove token

how do I uninstall the Software Tools?

For maintenance or troubleshooting purposes, your IT administrator may ask you to uninstall the Software Tools from your device.

You must have **administrator** rights on your Windows PC to uninstall the Software Tools.

- **Windows XP:** from the Windows taskbar, select "Start", "Settings", "Control Panel", "Add or Remove Programs", "SafeNet Authentication Service Software Tools". Click on "Remove" to run the Software Tools uninstaller and follow the instructions.
- **Windows 7:** from the Windows taskbar, select "Start", "Control Panel", "Programs and Features" option, "SafeNet Authentication Service Software Tools". Right-click on "Uninstall" to run the Software Tools uninstaller and follow the instructions.

Software Tools uninstaller does not delete the location where your MP token files are stored. After performing a new install of the Software Tools, you will be able to use them without enrolling again.

MP token for OSX Lion

In this chapter, you will find instructions for installing, activating and managing your MP token on Mac devices running OS X Lion.

The advantage of software tokens is mass deployment without hardware distribution. By thoughtful selection of the type of device upon which a software token can be installed, administrators can lock an end-user to a specific machine, limit the end-user to using only secure platforms or provide complete machine independence.

With our Secure Authentication service, MP tokens can be issued, revoked and reissued without restriction or the need to recover the MP token from the end-user. Multiple MP software tokens can be installed on a single device (e.g. hard drive) provided the usernames are unique.

what is a MP token?

Up until now, you've logged on with your User Name and Password. The problem is that passwords are easily compromised, putting your identity and the resources you access at risk. By using a MP token, you will be able to generate a "One-time Password" or "OTP". As the name implies, an OTP can only be used once. Each time you logon you will use your MP to generate a new OTP.

how does it protect me?

Password theft is the single most common way thieves and hackers steal identities and gain unauthorized access to networks and resources. While they have many ways to steal a password, success depends on the stolen password being valid, much the way credit card theft relies on the card being usable until you report it as stolen. The problem of course is that it is almost impossible for you or the security professionals that manage your network to discover your password has been compromised until long after damage has been done.

The MP token solves this problem because the instant you logon with your OTP, it is no longer valid. Any attempt to logon by reusing the OTP will not only fail, but also instantly alert your network security professionals to a possible attack on your identity.

can anybody use my MP token?

Thanks to PIN Code protection, your MP token is protected against unauthorized use by a PIN Code only you know. Again, much like a bank card or "Chip and PIN" credit card, the thief not only needs access to your MP token but must know your PIN Code as well. Any attempt to use the MP token with and incorrect PIN Code will fail. Successive attempts to guess your PIN Code will automatically "lock" your MP token, effectively disabling it, giving you and your network security professionals time to deal with the threat.

what kind of PIN Code is supported by MP token?

- **Server-side user-selected PIN Code:** the PIN Code is stored and managed at the Secure Authentication server level. You have the ability to change it at any time. Token Codes are generated without entering any PIN Code in the "Token" application (OTP=PIN Code+Token Code).
- **Server-side fixed PIN Code:** the PIN Code is stored and managed at the Secure Authentication server level. The PIN Code displayed during MP token installation is permanent, you can not change it. Token Codes are generated without entering any PIN Code in the "Token" application (OTP=PIN Code+Token Code).
- **Client-side user-selected PIN Code:** the PIN Code is stored and managed at the Mac level. You have the ability to change it at any time. The PIN Code must be entered into the "Token" application to generate a Token Code (OTP=Token Code).
- **Client-side fixed PIN Code:** the PIN Code is stored and managed at the Mac level. The PIN Code displayed during MP token installation is permanent, you can not change it. The PIN Code must be entered into the "Token" application to generate a Token Code (OTP = Token Code).

what is the “MP” application?

The “MP” application allows you to:

- select a MP token when several are installed
- generate a Token Code from this MP token
- rename this MP token
- resynchronize this MP token
- change the PIN Code of this MP token (when client-side PIN Code type is used)
- unlock this MP token when the feature is allowed by your Secure Authentication service administrators.
- retrieve the serial number of this MP token
- remove this MP token from your device

what are my responsibilities?

Using the MP token will not only provides security, it will simplify your life be reducing or eliminating the need to remember or periodically change passwords. Your MP token will do this for you, every time you logon. However, you do have a few simple obligations.

protect your PIN Code

You have to protect your PIN Code just as you would the PIN Code for your bank or credit card. Never share it with anybody, including people you trust. Your usual help desk will never ask for your PIN Code and you should never reveal it to them. Never write down your PIN Code.

what if I forget my PIN Code?

Contact your usual help desk. Upon verifying your identity they will be able to reset your PIN Code.

what if my MP token is locked?

Contact your usual help desk. Upon verifying your identity they will be able to unlock your MP token.

how long will my MP token continue to operate?

Your MP token will be able to generate OTPs until it is revoked by IT administrators.

what should I do if I can't logon using my token?

The most common cause of failed logon is entering an incorrect OTP. Never attempt to reuse a Token Code and ensure that you enter the Token Code exactly as displayed on the token, including any upper and lower case letters and punctuation that it may contain.

By default, your account will automatically lock for 15 minutes if more than 3 consecutive logon attempts fail. You must wait this amount of time before your account will unlock. Contact your usual help desk to resolve logon problems.

how do I enroll with a MP token?

how do I access the enrollment web site?

Within your e-mail client: open the "SAS Self-enrollment" message 1, and click on the self-enrollment URL link 2: your favorite Web browser (here Safari) will connect to the Secure Authentication enrollment web site.

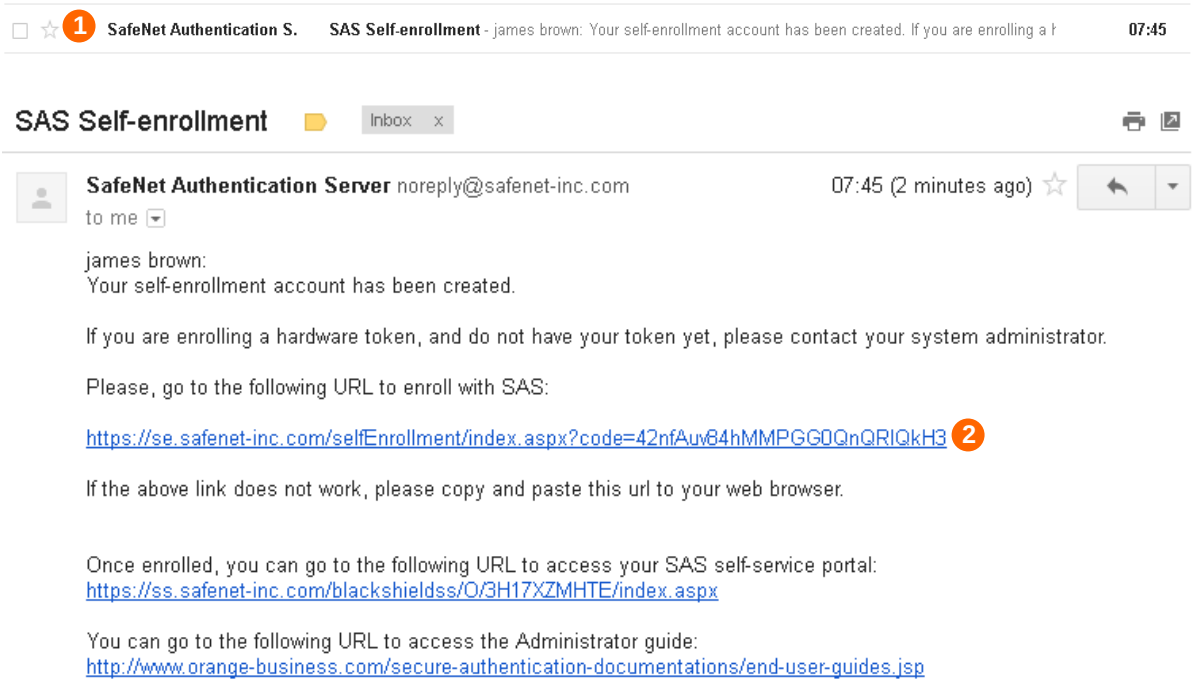

Figure 23: self-enrollment link

- **"SAS Self-enrollment" e-mail not received:** verify if the mail is not stored in the "junk" folder of your e-mail client.
- **"Your provisioning task has already been completed" error message:** verify you opened the latest self-enrollment message, and not an old one.

how do I select a Mac as target device?

Within your Safari browser: select “Mac OS X Lion” 1, click on “Next” 2, read displayed instructions 3 before closing your browser.

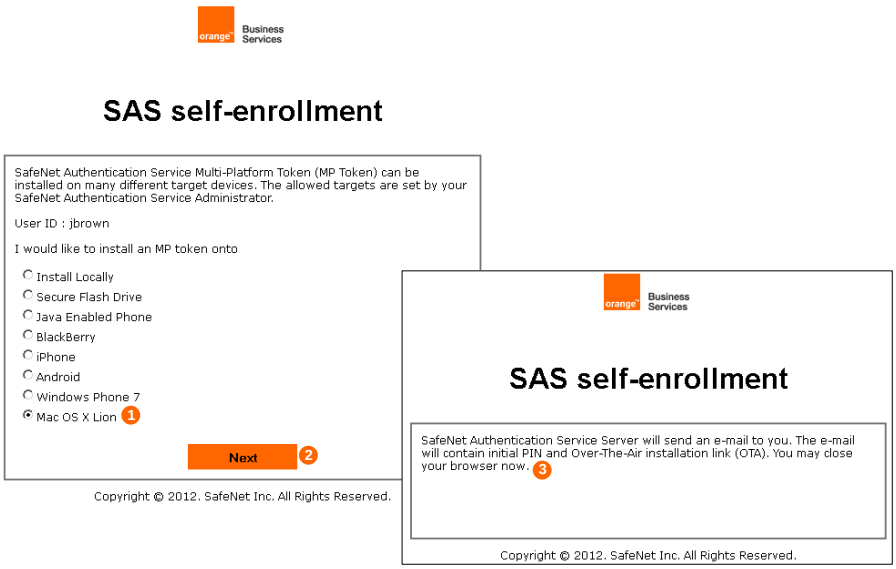

Figure 24: select Mac as target device

how do I download the “MP” application

Within your e-mail client: open the “Token Installation for Mac OS X” message 1, click on “https://se.safenet-inc.com/selfEnrollment/MP-1.pkg” link 2.

Within your Safari browser: in the upper right corner, click on the down arrow to display downloads 3, then click on “MP-1.pkg” file 4 to run the MP application installer.

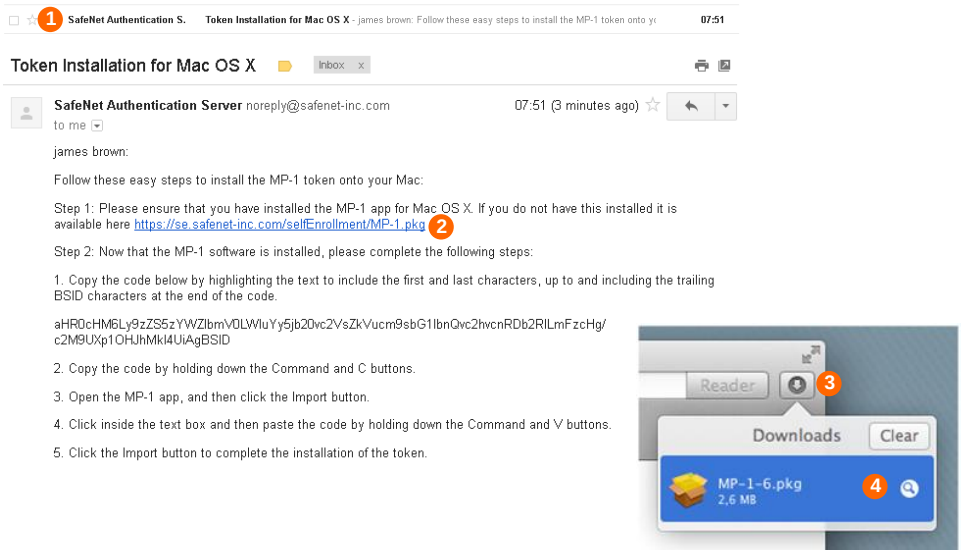

Figure 25: download “MP” application

how do I install the “MP” application?

Within your “MP” application installer: click on “Continue” ❶ (to accept the installer certificate), on “Continue” two times ❷❸, on “Agree” ❹ (to accept the software license agreement), on “Continue” ❺, select your “Macintosh HD” as destination ❻, click on “Continue” ❼, on “Install” ❽, then on “Close” at the end of the installation ❾.

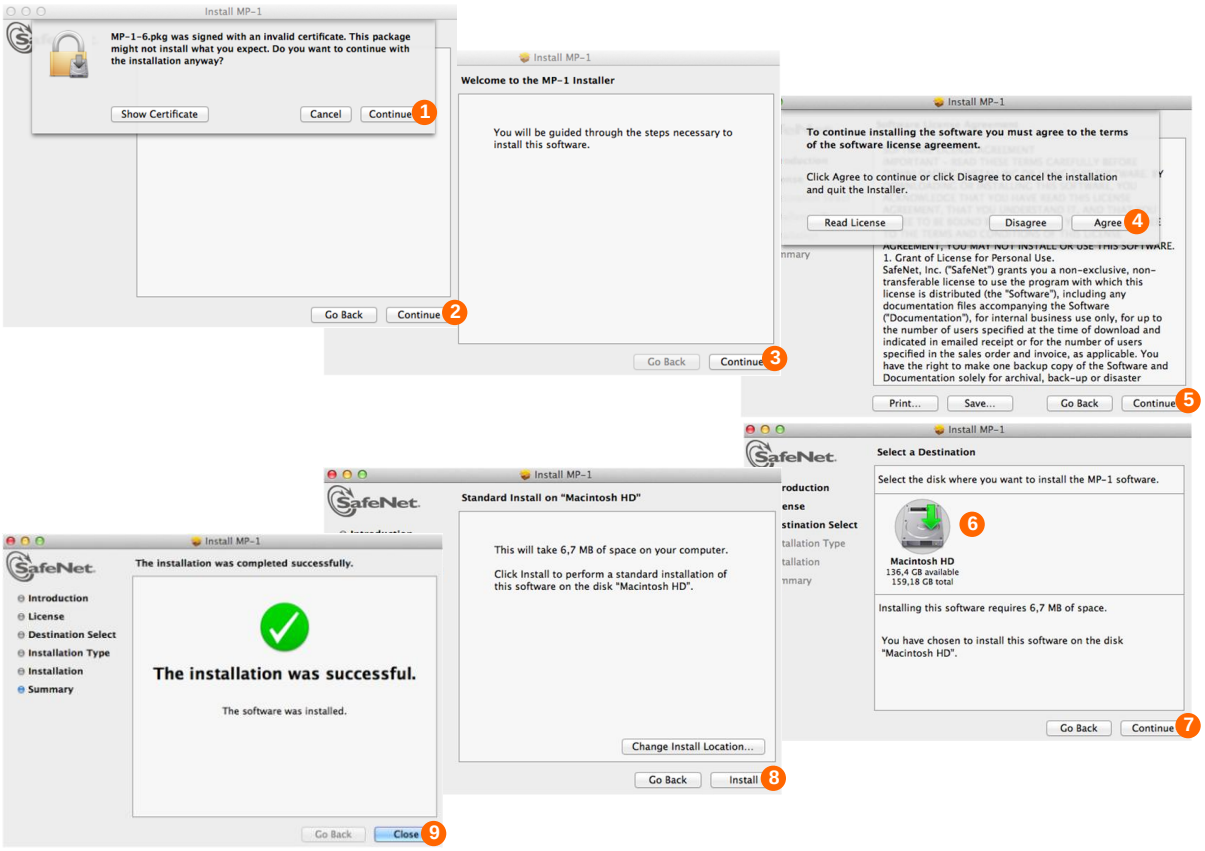

Figure 26: install “MP” application

how do I download and install my MP token file?

Within your e-mail client: open again the "Token Installation for Mac OS X" message, follow the Step 2 instructions to copy the MP token file code 1.

Within your finder: select "Application", then click on "MP-1.app" 2 to launch your "MP" application.

Within your "MP" application: click on "Paste" 3 to paste your MP token file code, then click on "Continue" 4

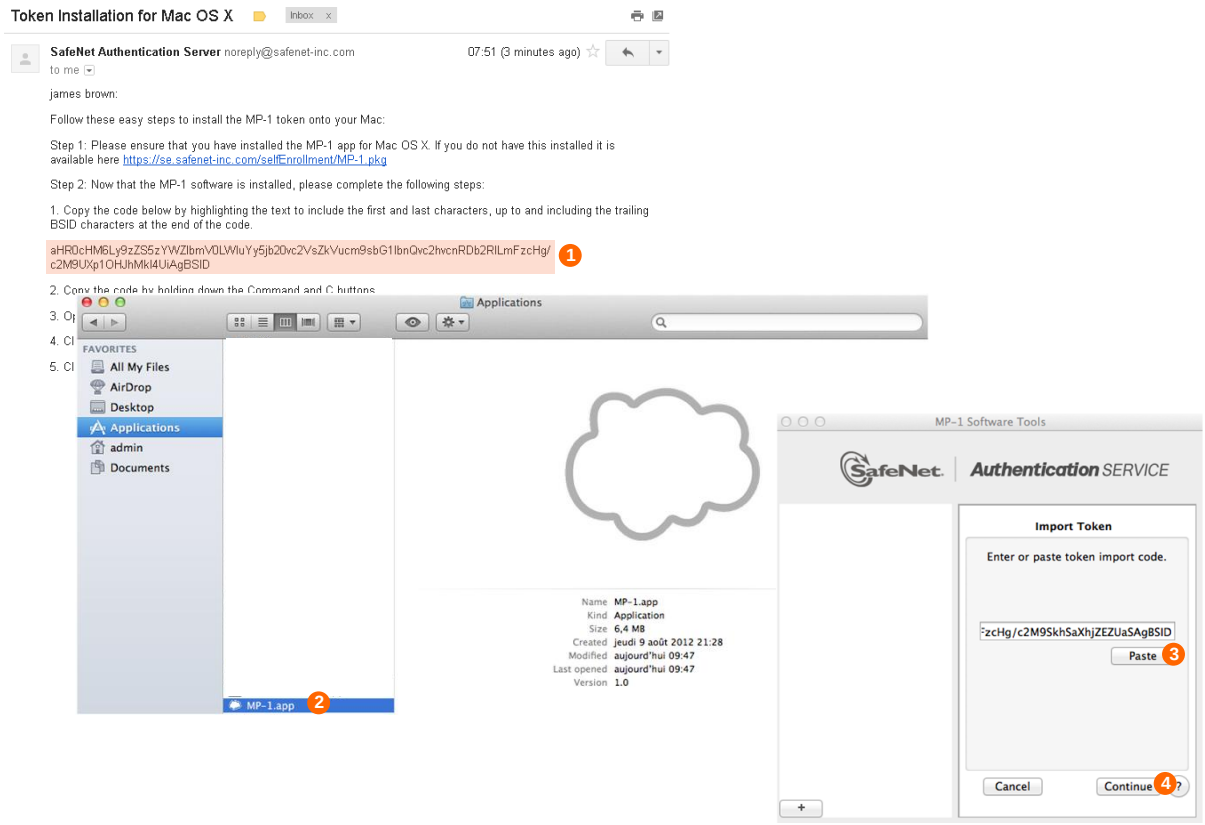

Figure 27: install MP token file

The end of the MP token file installation process depends on the type of the MP Token PIN Code.

how do I complete installation process with fixed PIN code

Within your "MP" application: memorize the displayed PIN Code ❶ (this will be your definitive PIN Code), then click on "Continue" ❷. A new entry appears in the left panel of your "MP" application confirming your MP token has been successfully activated. Memorize your User ID ❸.

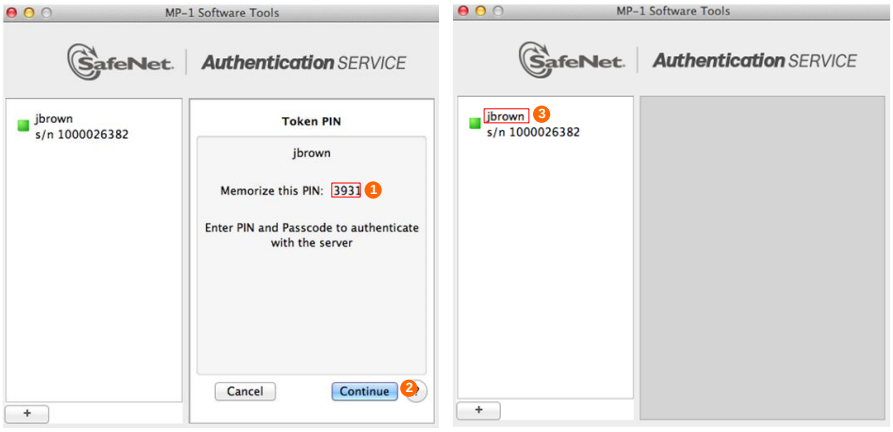

Figure 28: install MP token file with fixed PIN Code

how do I complete installation process with user-selected PIN code

Within your "MP" application: choose your PIN Code and enter it in the "Enter PIN" and "Re-enter PIN" fields ❶, then click on "Continue" ❷. A new entry appears in the left panel of your "MP" application confirming your MP token has been successfully activated. Memorize your User ID ❸.

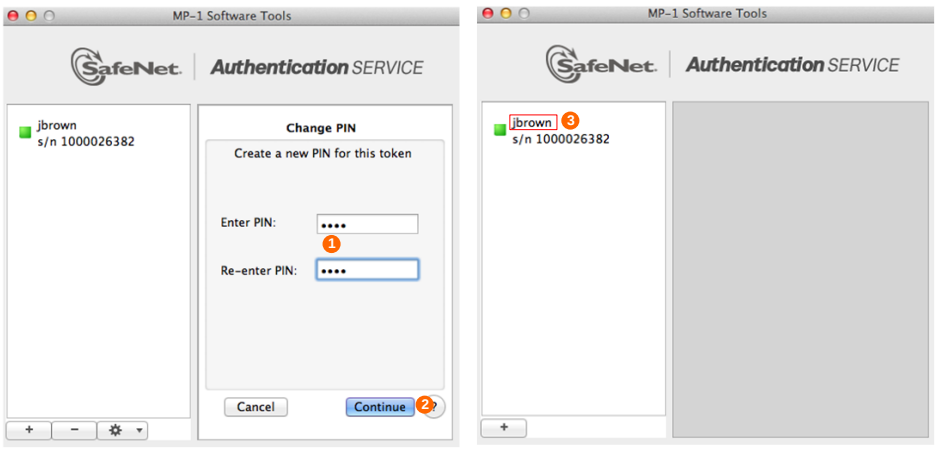

Figure 29: install MP token file with user-selected PIN Code

- **"PIN change failed" error message:** try to enter your new PIN Code again making sure to meet complexity requirements displayed.
- **"You have failed to provide the correct response too many times" error message:** contact your usual help desk.

how do I launch the MP application?

From the Mac Finder: select “Applications”, then “MP-1.app”.

how do I authenticate with my MP token?

You have the ability to test authentication with your MP token thanks to the SAS self-service portal.

4. **Within your e-mail client:** open the “SAS Self-enrollment” message 1 again, and click on the SAS self-service portal URL link 2: your web browser will connect to the self-service web site.

5. **Within the SAS self-service portal:** within the “Home” page click on “Sign In” 3, within the “Authenticate” page click on “Sign in using your token” 4.

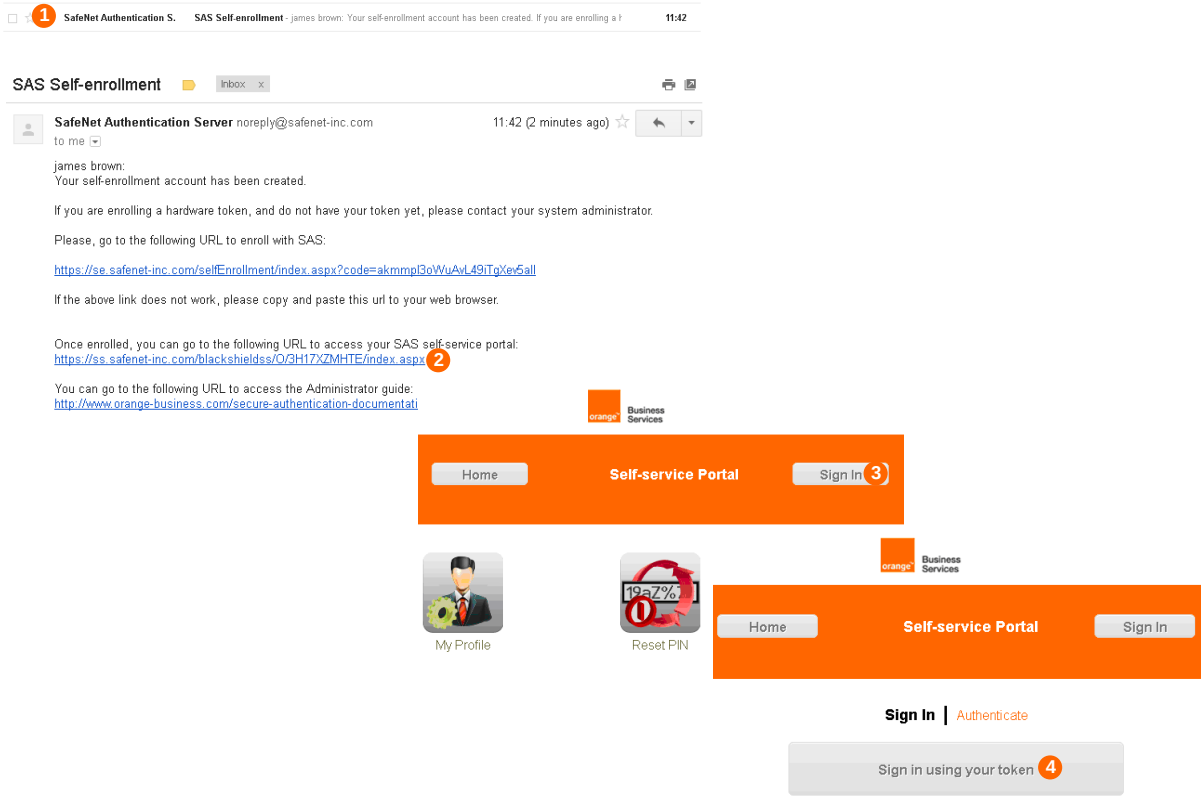

Figure 30: access to the SAS self-service portal sign in page

The authentication process depends on the type of the MP token PIN Code

Server-side PIN Code

1. **Within the SAS self-service portal:** within the "Authenticate to Process" page enter your user ID in the "User ID" field ❶ and your PIN Code in the "OTP" field ❷.

2. **Within your "MP" application:** click on the tile of the MP token you want to use ❸, then on "Copy" ❹ to copy the generated Token Code.

3. **Within the SAS self-service portal:** within the "Authenticate to Process" page paste the Token Code value next to the PIN Code in the "OTP" field ❺, then click on "OK" ❻. The "Sign Out" button ❼ displayed within the "Home" page indicates your authentication is successful.

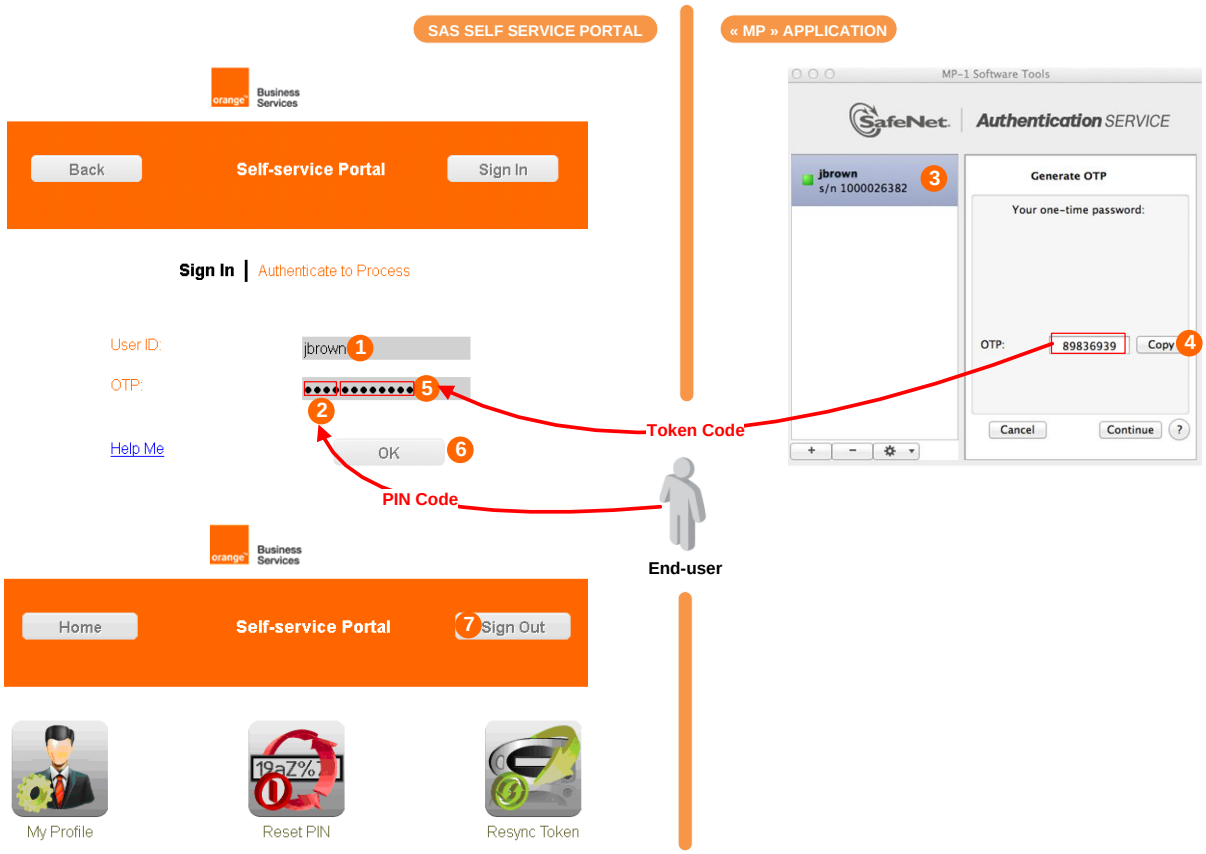

Figure 31: authenticate (with server-side PIN Code)

"Your login attempt was not successful" error message: try to authenticate again, making sure to enter your PIN Code followed by the Token Code generated by your MP token in the "OTP" field.

client-side PIN Code

1. **Within the SAS self-service portal:** within the "Authenticate to Process" page enter your user ID in the "User ID" field ❶.

2. **Within your "MP" application:** click on the tile of the MP token you want to use ❷, enter your PIN Code in the "PIN" field ❸, click on "Continue" ❹, then on "Copy" ❺ to copy the generated Token Code.

3. **Within the SAS self-service portal:** within the "Authenticate to Process" page paste the Token Code value in the "OTP" field ❻, then click on "OK" ❼. The "Sign Out" button ❽ displayed within the "Home" page indicates your authentication is successful.

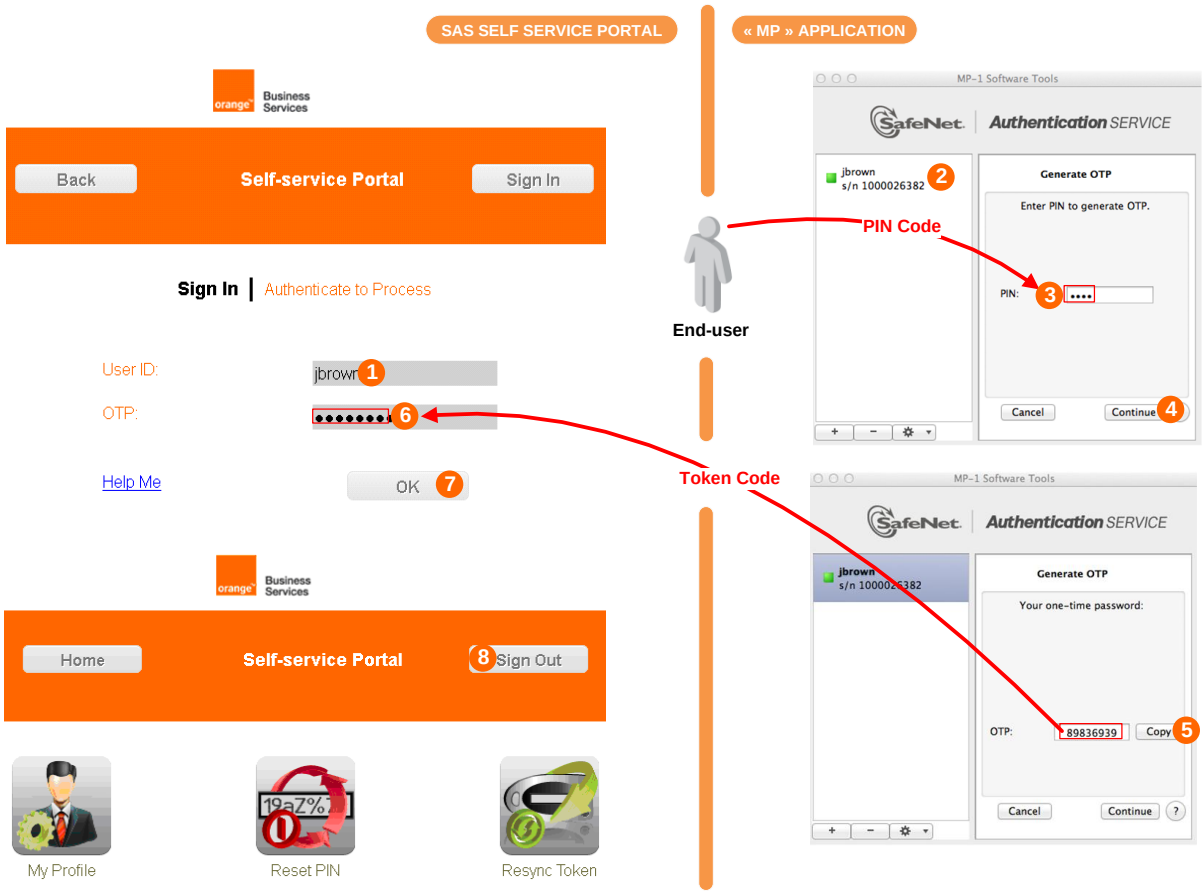

Figure 32: authenticate (with client-side PIN Code)

- **"Your login attempt was not successful" error message:** try to authenticate again, making sure to enter only the Token Code generated by your MP token in the "OTP" field.

how do I change my PIN Code?

The PIN Code change process depends on the type of the MP token PIN Code

server-side PIN Code

Within the SAS self-service portal: within the "Home" page, once authenticated ("Sign Out" button must be displayed 1), click on "Reset PIN" 2, within the "Create New PIN" page choose a new PIN Code and enter it in the "Create New PIN" and "Verify PIN" fields 3, then click on "OK" 4. Within the "Create New PIN" page a message indicates your PIN Code change is successful 5.

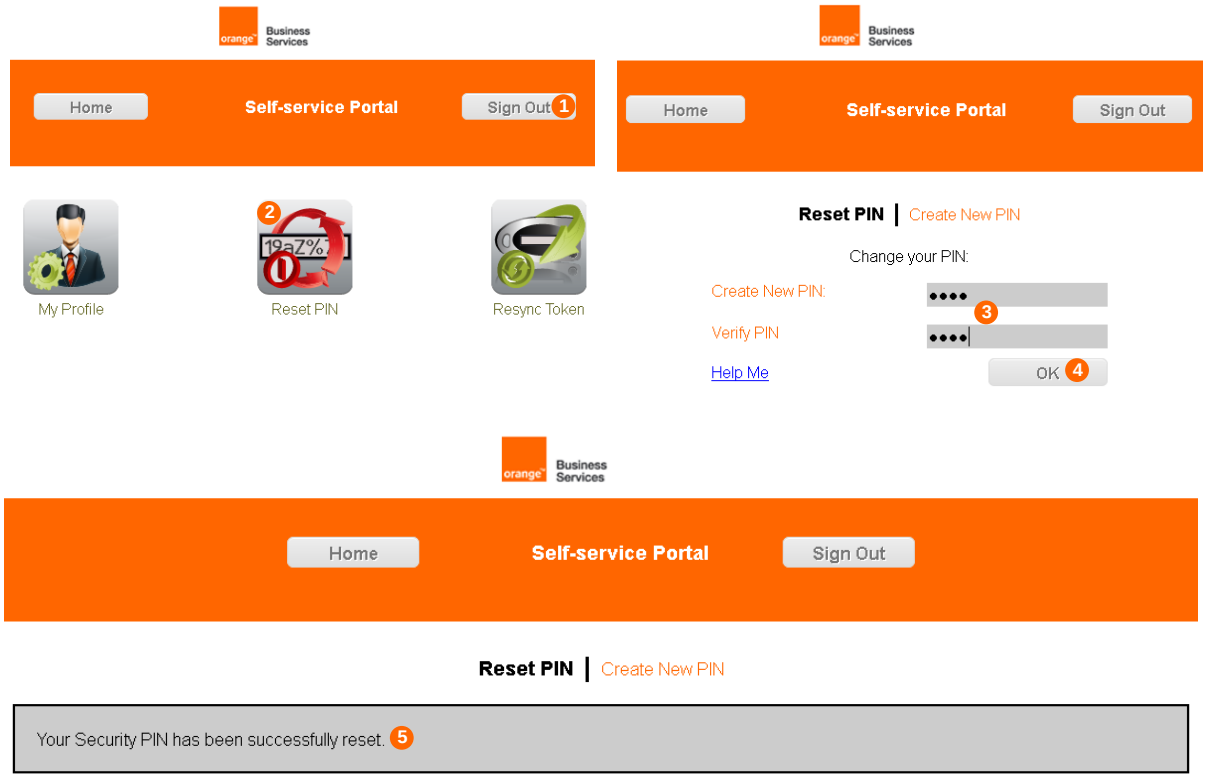

Figure 33: change server-side PIN Code

- **"No tokens are enabled to change the Personal Identification Number (PIN)" error message:** your MP token has not a server-side PIN Code but a client-side instead.

client-side PIN Code

Within your "MP" application: click on the tile of the MP token you want to use, select the gear icon, then "Change PIN" 1, enter your current PIN Code in the "Current PIN" field 2, choose a new PIN Code and enter it in the "New PIN" and "Verify New PIN" fields 3, then click on "Continue" 4. In the right panel of your "MP" application a message indicates your PIN Code change is successful 5.

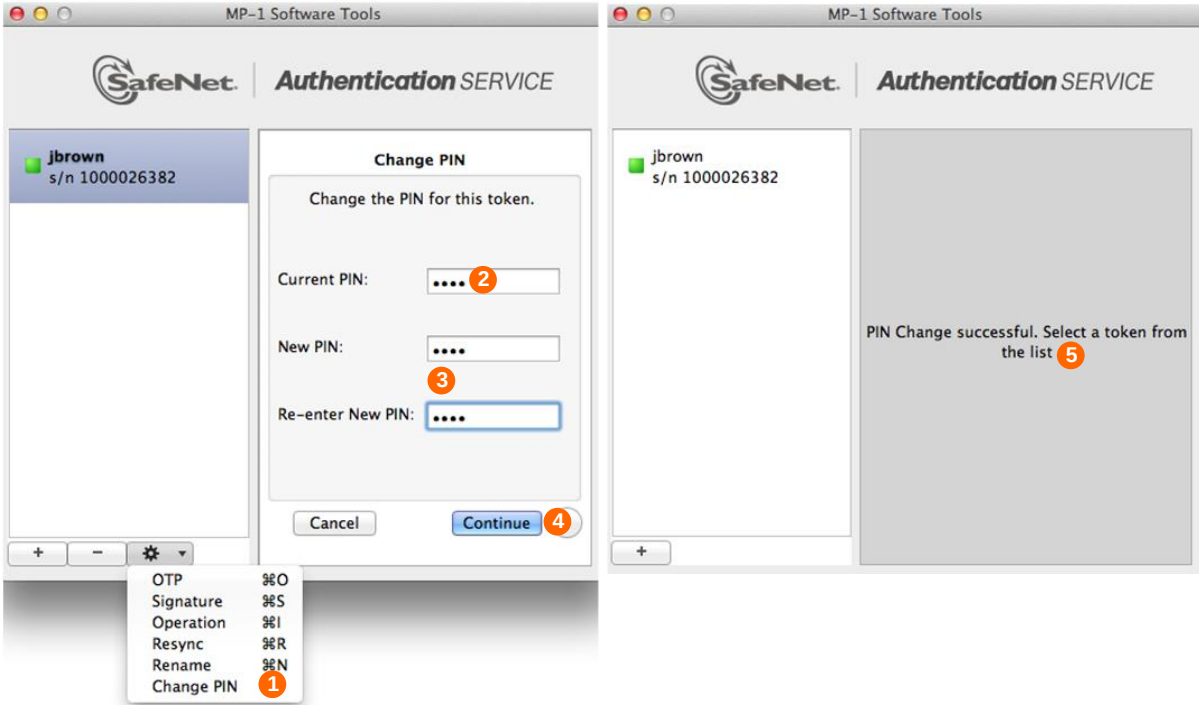

Figure 34: change client-side PIN Code

- **"PIN Change Failed" error message:** try to change your PIN Code again, making sure to enter a complex one, the correct number of characters, and the correct types **of character.**

how do I resynchronize my MP token?

Within the SAS self-service portal: within the “Home” page click on “Resync Token” ❶, within the “User” page enter your user ID in the “User ID” field ❷, click on “Next” ❸ , enter the serial of your MP token in the “Serial” field ❹, then click on “Next” ❺.

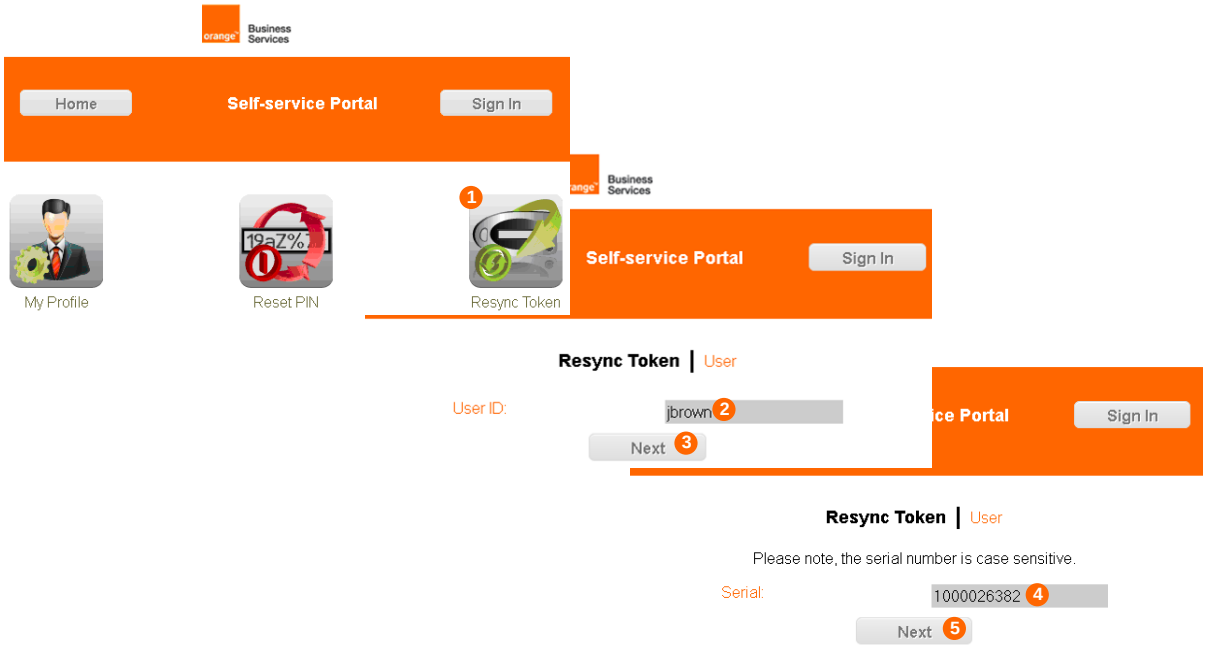

Figure 35: resynchronize token (common part)

The end of the resynchronization process depends on the type of the MP token PIN Code

server-side PIN Code

4. **Within the SAS self-service portal:** within the "Challenge/Response" page copy the "Respond to challenge" value 1.

5. **Within your "MP" application:** click on the tile of the MP token you want to use, select the gear icon, then "Resync" 2, paste the challenge value in the "Challenge" field 3, click on "Continue" 4, then click on "Copy" 5 to copy the generated response.

6. **Within the SAS self-service portal:** within the "Challenge/Response" page paste the response value in the "Response" field 6, then click on "OK" 7. Within the "Confirmation" page a message indicates your token resynchronization is successful 8.

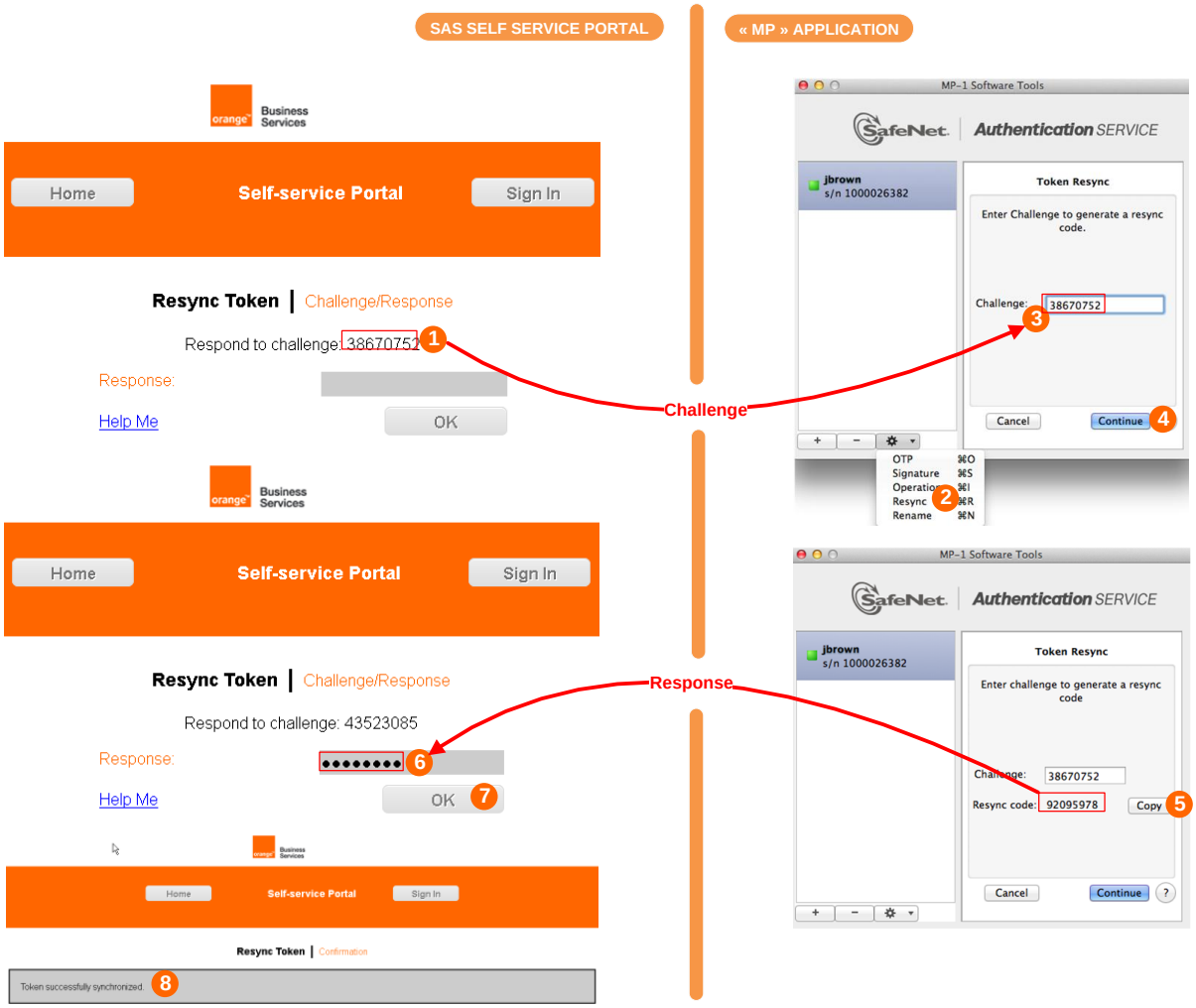

Figure 36: resynchronize token (with server-side PIN Code)

- **"The token cannot be synchronized" error message:** try to resynchronize your MP token again, making sure to copy/paste the right challenge/response values.

client-side PIN Code

7. **Within the SAS self-service portal:** within the "Challenge/Response" page copy the "Respond to challenge" value ❶.

8. **Within your "Token" application:** click on the tile of the MP token you want to use, select the gear icon, then "Resync" ❷, enter you PIN Code in the "PIN" field ❸, click on" Continue" ❹, paste the challenge value in the "Challenge" field ❺, click on "Continue" ❻, then click on "Copy" to copy the generated response ❼.

9. **Within the SAS self-service portal:** within the "Challenge/Response" page paste the response value in the "Response" field ❽, then click on "OK" ❾. Within the "Confirmation" page a message indicates your token resynchronization is successful ❿.

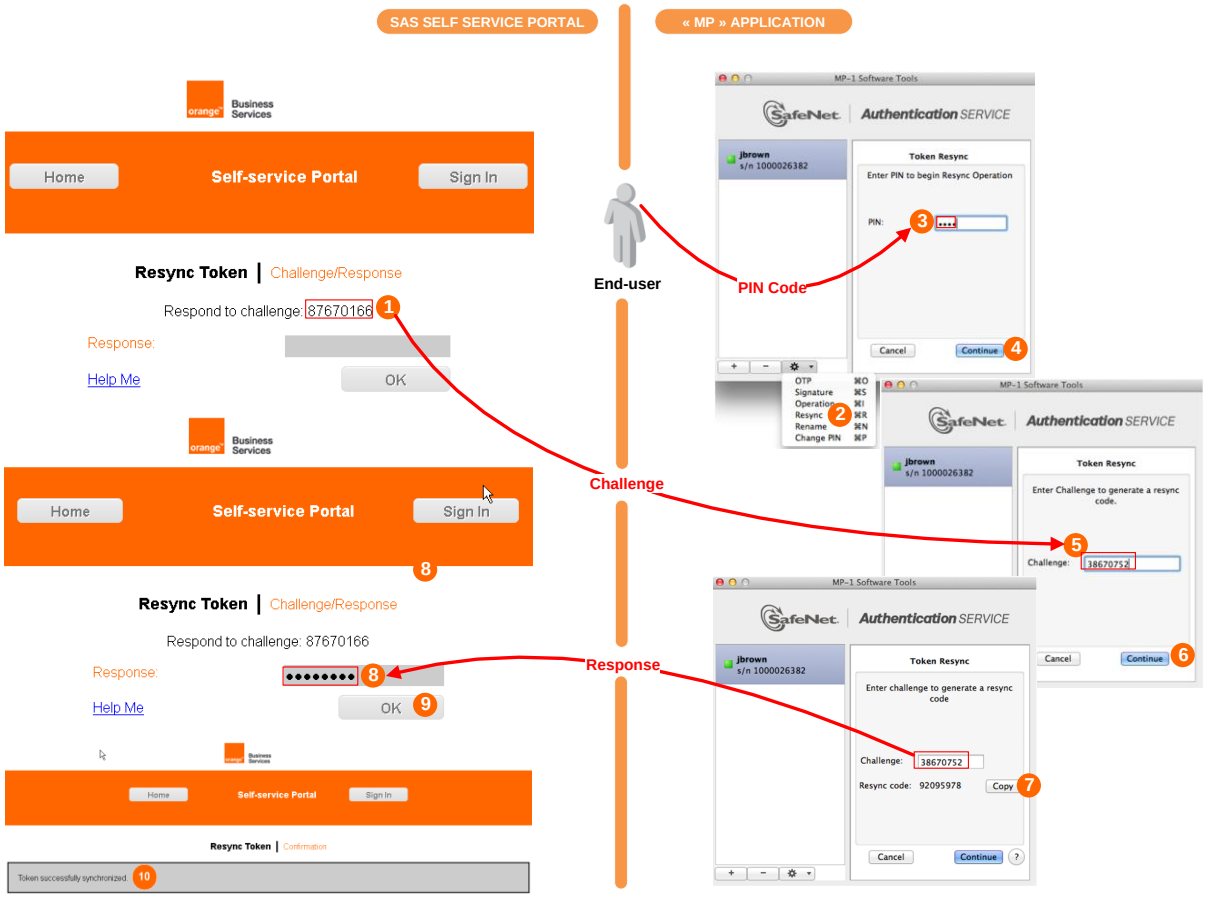

Figure 37: resynchronize token (with client-side PIN Code)

- **"The token cannot be synchronized" error message:** try to resynchronize your MP token again, making sure to copy/paste the right challenge/response values.

- **If the self-service portal displays the "The token cannot be synchronized" message :**
  Try to resynchronize your MP token again, making sure to copy/paste the right challenge/response values.

how do I rename my MP token?

By default, MP token name is based on your user ID.

Within your "MP" application: click on the tile of the MP token you want to use, select the gear icon, then "Rename" ❶, enter your PIN Code in the "PIN" field ❷, click on "Continue" ❸, enter the new MP token name in the "New Name" field ❹, then click on "Continue" ❺. Your MP token is now referenced with the new name ❻.

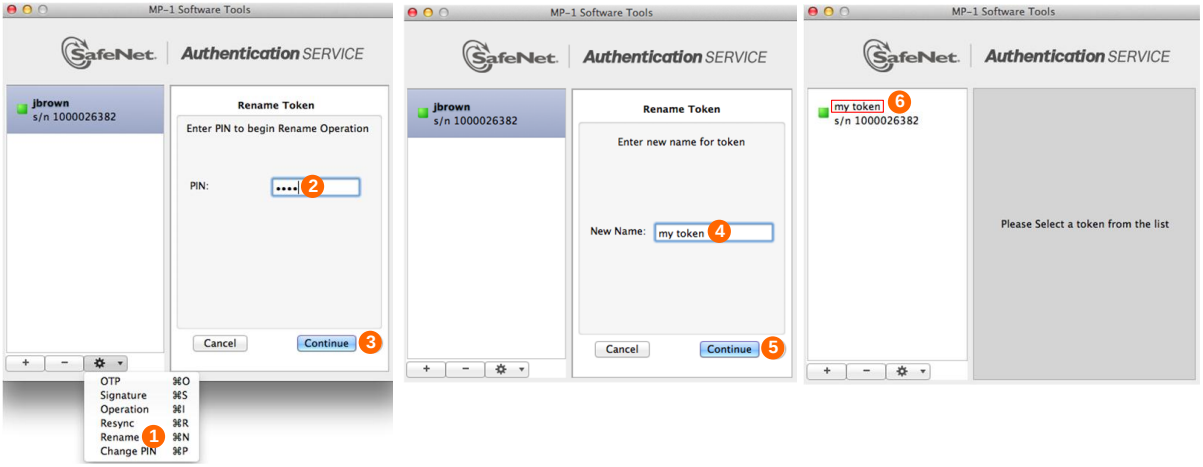

Figure 38: rename token

how do I retrieve my MP token serial?

Within your "MP" application: memorize the serial value displayed within the tile of your MP token ❶.

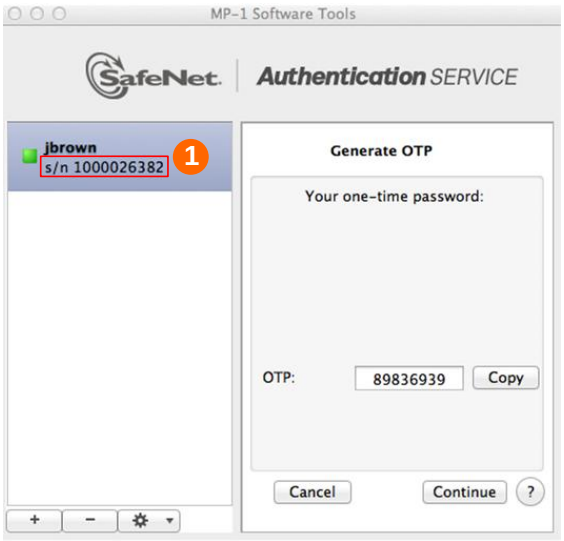

Figure 39: retrieve token serial

how do I retrieve the “Token” application version?

For maintenance or troubleshooting purposes, your IT administrator may ask you the version of your Token application MP.

Within your finder: select “Application”, then “MP-1.app” 1. Memorize the “MP” application version 1.

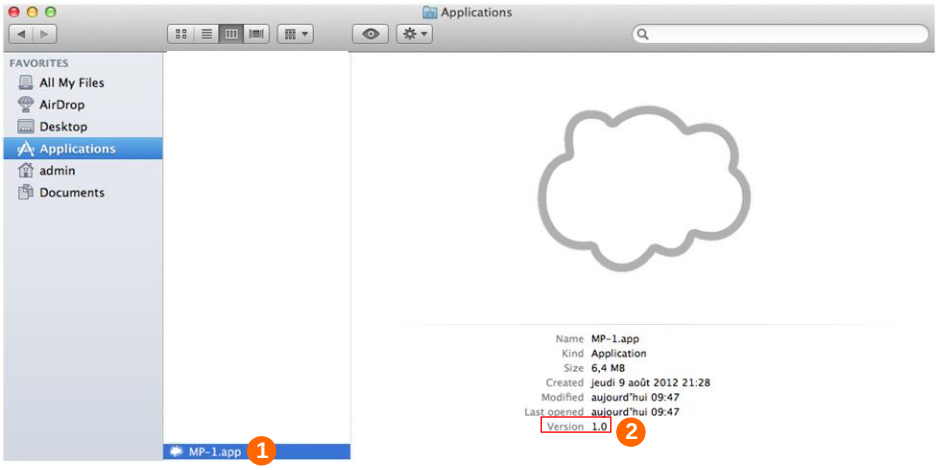

Figure 40: retrieve “Token” application version

how do I remove my MP token?

For maintenance or troubleshooting purposes, your IT administrator may ask you to remove a MP token from your device.

Within your “MP” application: click on the tile of the MP token you want to use, select the minus icon 1, check the “Remove Token box 2, then click on “Continue” 3.The token has been successfully removed 4. In the right panel of your “MP” application a message indicates your MP token deletion is successful 5.

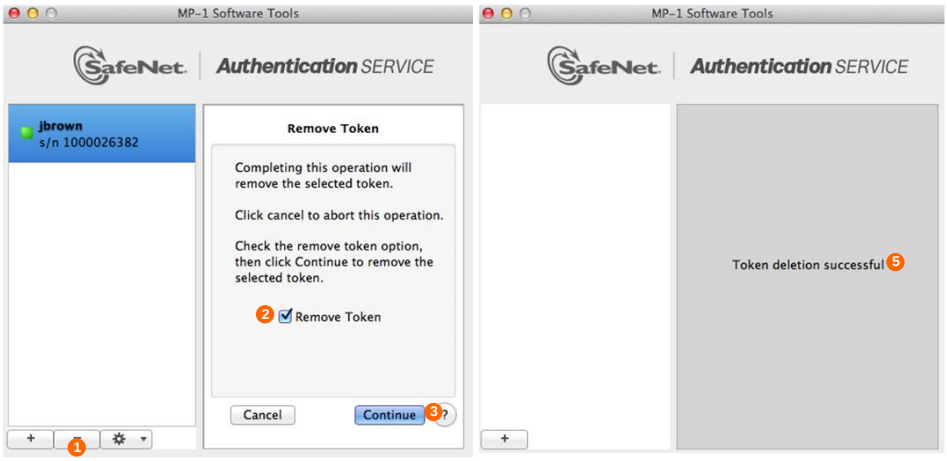

Figure 41: remove token

MP token for iPhone

In this chapter, you will find instructions for installing, activating and managing your MP token for iPhone.

The advantage of software tokens is mass deployment without hardware distribution. By thoughtful selection of the type of device upon which a software token can be installed, administrators can lock an end-user to a specific machine, limit the end-user to using only secure platforms or provide complete machine independence.

With our Secure Authentication service, MP tokens can be issued, revoked and reissued without restriction or the need to recover the MP token from the end-user. Multiple MP software tokens can be installed on a single device (e.g. hard drive) provided the usernames are unique.

what is a MP token?

Up until now, you've logged on with your User Name and Password. The problem is that passwords are easily compromised, putting your identity and the resources you access at risk. By using a MP token, you will be able to generate a "One-time Password" or "OTP". As the name implies, an OTP can only be used once. Each time you logon you will use your MP to generate a new OTP.

how does it protect me?

Password theft is the single most common way thieves and hackers steal identities and gain unauthorized access to networks and resources. While they have many ways to steal a password, success depends on the stolen password being valid, much the way credit card theft relies on the card being usable until you report it as stolen. The problem of course is that it is almost impossible for you or the security professionals that manage your network to discover your password has been compromised until long after damage has been done.

The MP token solves this problem because the instant you logon with your OTP, it is no longer valid. Any attempt to logon by reusing the OTP will not only fail, but also instantly alert your network security professionals to a possible attack on your identity.

can anybody use my MP token?

Thanks to PIN Code protection, your MP token is protected against unauthorized use by a PIN Code only you know. Again, much like a bank card or "Chip and PIN" credit card, the thief not only needs access to your MP token but must know your PIN Code as well. Any attempt to use the MP token with and incorrect PIN Code will fail. Successive attempts to guess your PIN Code will automatically "lock" your MP token, effectively disabling it, giving you and your network security professionals time to deal with the threat.

what kind of PIN Code is supported by MP token?

- **Server-side user-selected PIN Code:** the PIN Code is stored and managed at the Secure Authentication server level. You have the ability to change it at any time. Token Codes are generated without entering any PIN Code in the “MP” application (OTP=PIN Code+Token Code).
- **Server-side fixed PIN Code:** the PIN Code is stored and managed at the Secure Authentication server level. The PIN Code displayed during MP token installation is permanent, you can not change it. Token Codes are generated without entering any PIN Code in the “MP” application (OTP=PIN Code+Token Code).
- **Client-side user-selected PIN Code:** the PIN Code is stored and managed at the iPhone level. You have the ability to change it at any time. The PIN Code must be entered into the “MP“ application to generate a Token Code (OTP=Token Code).
- **Client-side fixed PIN Code:** the PIN Code is stored and managed at the iPhone level. The PIN Code displayed during MP token installation is permanent, you can not change it. The PIN Code must be entered into the “MP” application to generate a Token Code (OTP = Token Code).

what is the “MP” application?

The “MP” application allows you to:

- select a MP token when several are installed
- generate a Token Code from this MP token
- rename a MP token
- resynchronize a MP token
- change the PIN Code of a MP token (when client-side PIN Code type is used)
- retrieve the serial number of a MP token
- remove a MP token from your iPhone

You can download MP application from App Store for free.

what are my responsibilities?

Using the MP token will not only provides security, it will simplify your life be reducing or eliminating the need to remember or periodically change passwords. Your MP token will do this for you, every time you logon. However, you do have a few simple obligations.

protect your PIN Code

You have to protect your PIN Code just as you would the PIN Code for your bank or credit card. Never share it with anybody, including people you trust. Your usual help desk will never ask for your PIN Code and you should never reveal it to them. Never write down your PIN Code.

what if I forget my PIN Code?

Contact your usual help desk. Upon verifying your identity they will be able to reset your PIN Code.

what if my MP token is locked?

Contact your usual help desk. Upon verifying your identity they will be able to unlock your MP token.

how long will my MP token continue to operate?

Your MP token will be able to generate OTPs until it is revoked by IT administrators.

what should I do if I can't logon using my token?

The most common cause of failed logon is entering an incorrect OTP. Never attempt to reuse a Token Code and ensure that you enter the Token Code exactly as displayed on the token, including any upper and lower case letters and punctuation that it may contain.

By default, your account will automatically lock for 15 minutes if more than 3 consecutive logon attempts fail. You must wait this amount of time before your account will unlock. Contact your usual help desk to resolve logon problems.

how do I enroll with a MP token?

In this chapter, Safari Web browser is used. Please use e-mail client (and not browser/webmail) to access messages sent by the SAS.

how do I access the enrollment web site?

Within your e-mail client: open the "SAS Self-enrollment" message 1, and tap the self-enrollment URL link 2: your web browser will connect to the Secure Authentication enrollment web site.

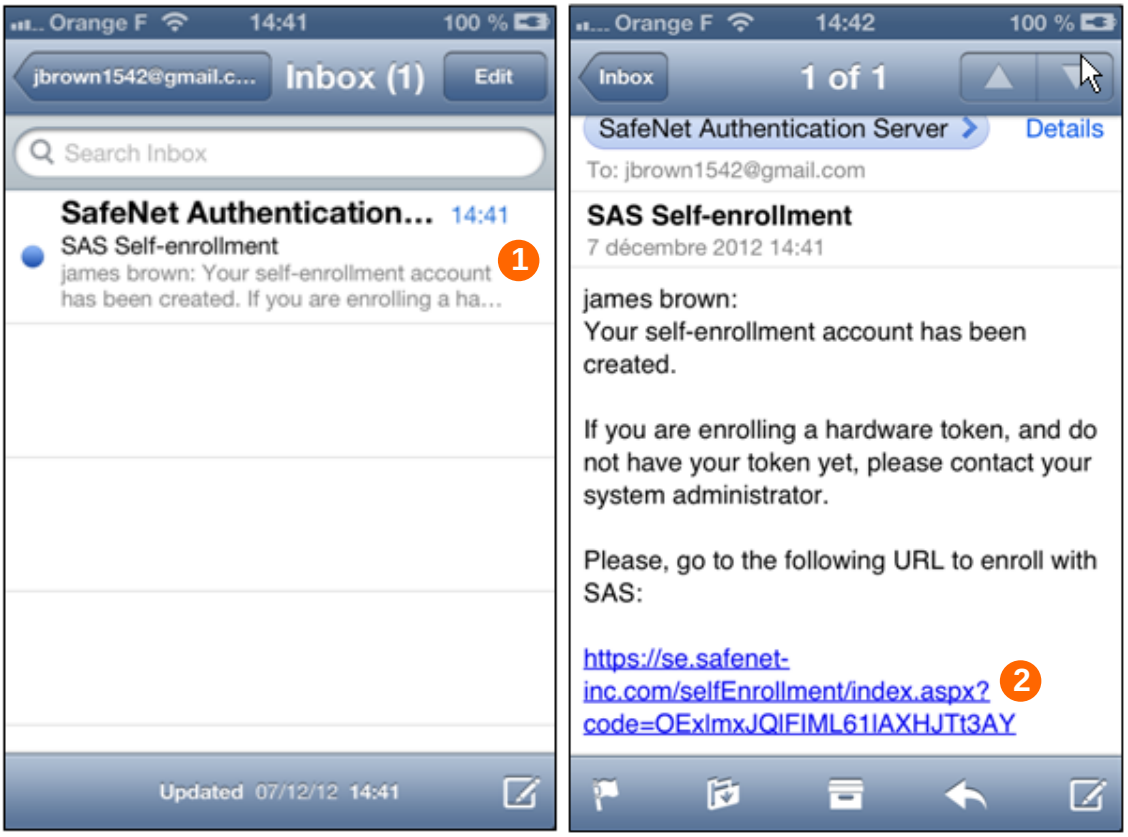

Figure 42: self-enrollment link

- **"SAS Self-enrollment" e-mail not received:** verify if the mail is not stored in the "junk" folder of your e-mail client.
- **"Your provisioning task has already been completed" error message:** verify you opened the latest self-enrollment message, and not an old one.

how do I select an iPhone as target device?

Within your Safari browser: tap “iPhone” ❶, click on “Next” ❷, read displayed instructions ❸ before closing your browser.

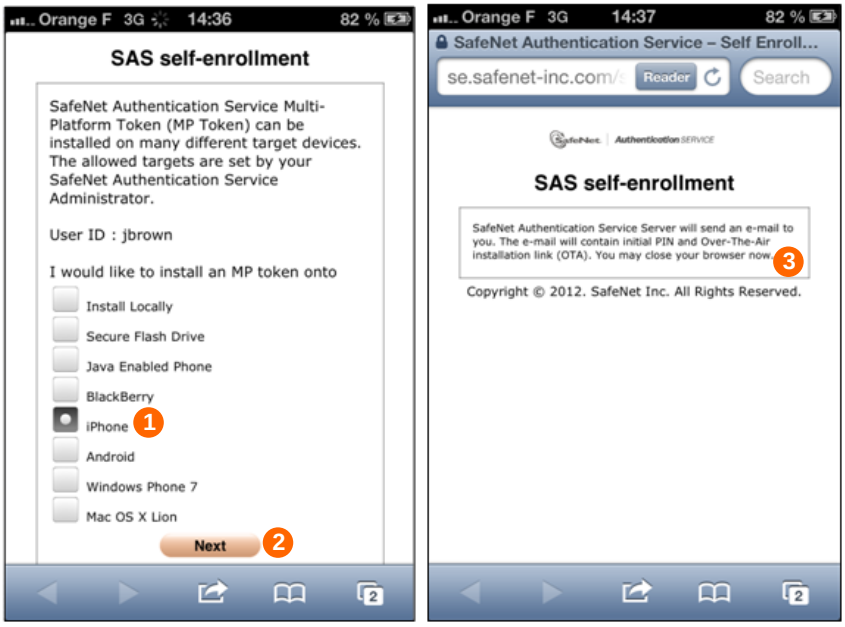

Figure 43: select iPhone as target device

how do I download the “MP” application?

1. **Within your e-mail client:** open the “Over-The-Air (OTA) Installation” message ❶, tap the icon related to the Apple iOS ❷ to retrieve the “MP” application from the App Store.
2. **Within the App Store:** tap “FREE” ❸ to download the “MP” application.

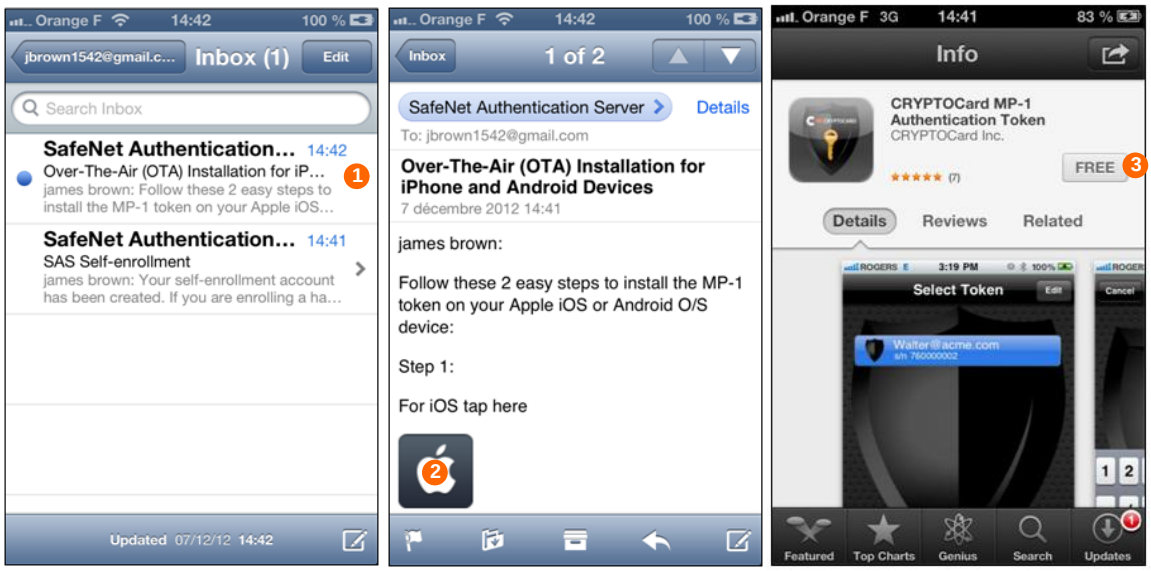

Figure 44: download “MP” application

how do I install the “MP” application?

1. **Within the App Store:** tap “INSTALL APP” ❶ to install the “MP” application on your iPhone.
2. **Within your iPhone home screen:** at the end of the installation, the “MP” application launch icon ❷ appears.

Figure 45: install "MP" application

how do I download the MP token file?

1. **Within your e-mail client:** open the “Over-The-Air (OTA) Installation” message ❶ again, tap the MP-1 token profile URL link ❷ to retrieve the “MP” application from the App Store.
2. **Within your Safari browser:** the MP token file (with “.7mp” extension) is now downloaded ❸.

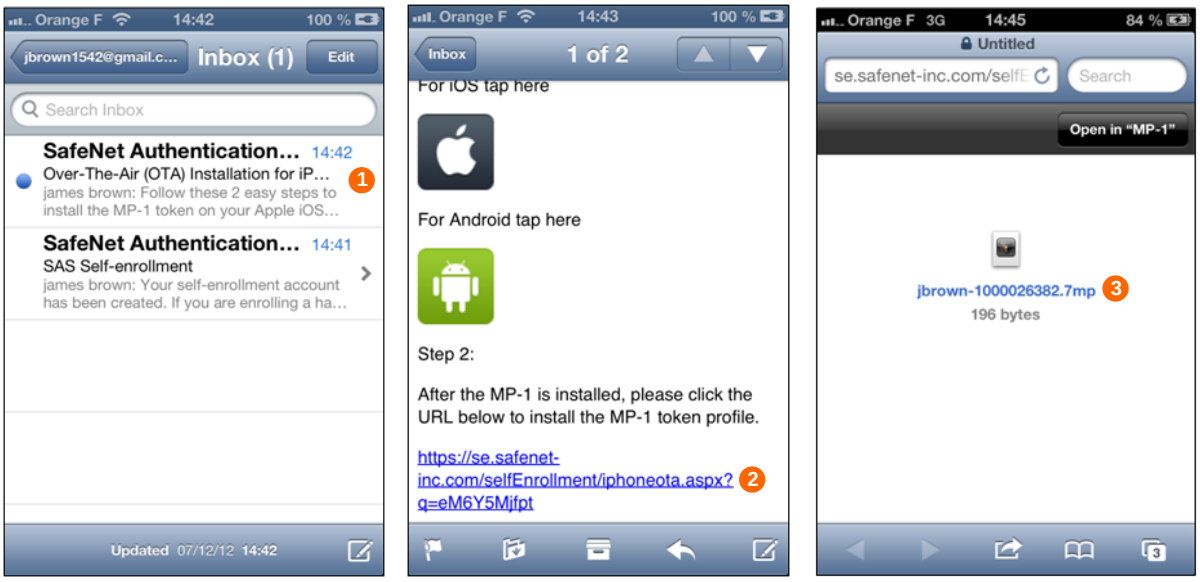

Figure 46: download token file

how do I install the MP token file with user-selected PIN Code?

1. **Within your Safari browser:** tap “Open in MP-1” ❶.
2. **Within your “MP” application:** choose your PIN Code and enter it the “Enter new PIN” field ❷, tap “Done” ❸, re-enter your PIN Code in the “Re-enter new PIN” field ❹, then tap “Done” ❺ to display the “Select Token” screen.

Figure 47: install token file (with user selected PIN Code)

- **“PIN change failed” error message:** try to enter your new PIN Code again making sure to meet complexity requirements displayed.
- **“You have failed to provide the correct response too many times” message:** contact your usual help desk.

how do I install the MP token file with fixed PIN Code?

1. **Within your Safari browser:** tap “Open in MP-1” 1.
2. **Within your “MP” application:** memorize the displayed PIN Code 2, tap “OK” 3, then “Cancel” 4 to display the “Select Token” screen.

Figure 48: install token file (with fixed PIN Code)

how do I launch the “MP” application?

Within your iPhone home screen: tap the “MP” application launch icon.

how do I select my MP token?

Within your “MP” application: within the “Select Token” screen, tap the tile of the MP token you want to select 1.

Figure 49: select token

how do I authenticate with my MP token?

You have the ability to test authentication with your MP token thanks to the SAS self-service portal.

1. **Within your e-mail client:** open the "SAS Self-enrollment" message 1 again, and tap the SAS self-service portal URL link 2: your web browser will connect to the self-service web site.

2. **Within the SAS self-service portal:** within the "Home" page tap "Sign In" 3, then within the "Authenticate" page tap "Sign in using your token" 4.

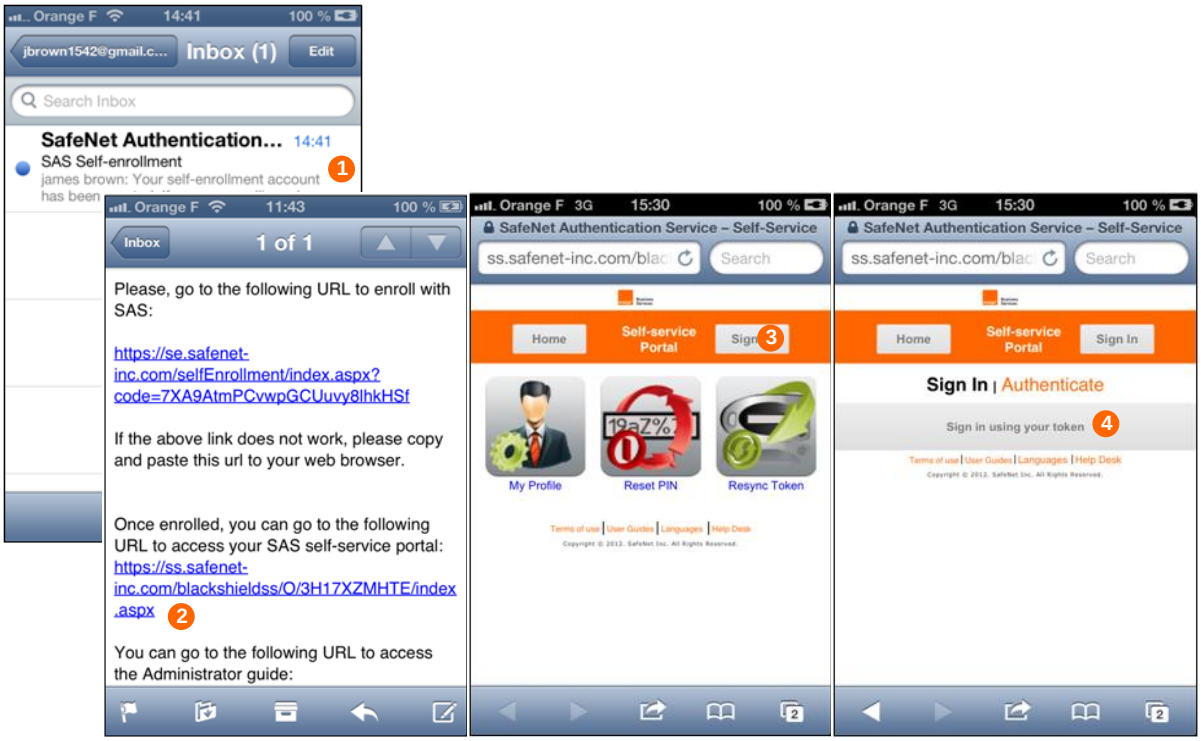

Figure 50: access to the SAS self-service portal sign in page

The authentication process depends on the type of the MP token PIN Code.

server-side PIN Code

1. **Within the SAS self-service portal:** within the "Authenticate to Process" page enter your user ID in the "User ID" field ❶ and your PIN Code in the "OTP" field ❷.

2. **Within your "MP" application:** within the "One-Time Password" screen copy the new generated Token Code value ❸ (hold your finger on the value until the "Copy" icon appears).

3. **Within the SAS self-service portal:** within the "Authenticate to Process" page paste the Token Code value next to the PIN Code in the "OTP" field ❹ (hold your finger on the field until the "Paste" icon appears), then tap "OK" ❺. The "Sign Out" button ❻ displayed within the "Home" page indicates your authentication is successful.

Figure 51: authenticate (with server-side PIN Code)

- **"Your login attempt was not successful" error message:** try to authenticate again, making sure to enter your PIN Code followed by the Token Code generated by your MP token in the "OTP" field.

client-side PIN Code

1. **Within the SAS self-service portal:** within the "Authenticate to Process" page enter your user ID in the "User ID" field ❶.

2. **Within your "MP" application:** enter your PIN Code in the "Enter PIN for token" field ❷, tap "Done" ❸, within the "One-Time Password" screen copy the new generated Token Code value ❹ (hold your finger on the value until the "Copy" icon appears).

3. **Within the SAS self-service portal:** within the "Authenticate to Process" page paste the Token Code in the "OTP" field ❺ (hold your finger on the field until the "Paste" icon appears), then click on "OK" ❻. The "Sign Out" button ❼ displayed within the "Home" page indicates your authentication is successful.

Figure 52: authenticate (with client-side PIN Code)

- **"Your login attempt was not successful" error message:** try to authenticate again, making sure to enter only the Token Code generated by your MP token in the "OTP" field.

how do I edit my PIN Code?

Within your "MP" application: within the "Select Token" screen, tap the tile of the MP token you want to edit ❶, tap "Edit" ❷, then tap the tile of the MP token again ❸ to display the "Edit Token" screen.

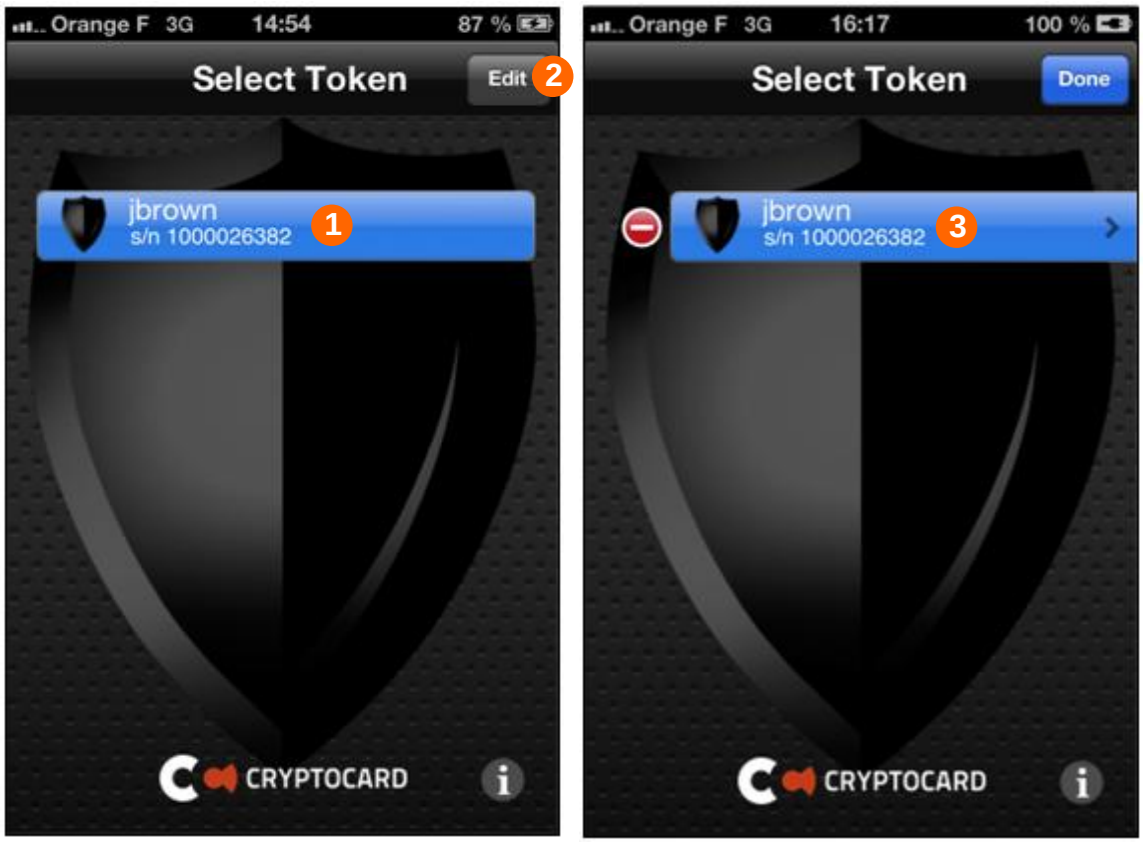

Figure 53: edit token

how do I change my PIN Code?

The PIN Code change process depends on the type of the MP token PIN Code.

server-side PIN Code

Within the SAS self-service portal: within the "Home" page, once authenticated ("Sign Out" button must be displayed 1), tap "Reset PIN" 2, within the "Create New PIN" page choose a new PIN Code and enter it in the "Create New PIN" and "Verify PIN" fields 3, then tap "OK" 4. Within the "Create New PIN" page a message indicates your PIN Code change is successful 5.

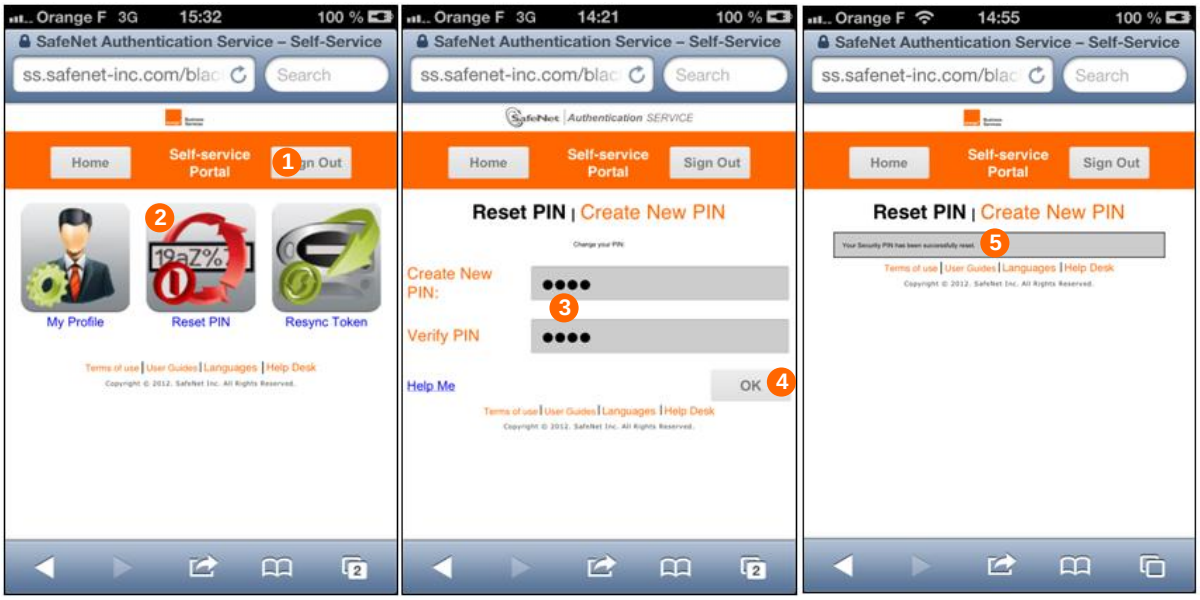

Figure 54: change server-side PIN Code

- **"No tokens are enabled to change the Personal Identification Number (PIN)" error message:** your MP token has not a server-side PIN Code but a client-side instead.

client-side PIN Code

Within your "MP" application: within the "Edit Token" screen tap "Change PIN" 1, choose a new PIN Code and enter it in the "Enter new PIN" field 2, tap "Done" 3, re-enter your new PIN Code in the "Re-enter new PIN" field 4, then tap "Done" 5.

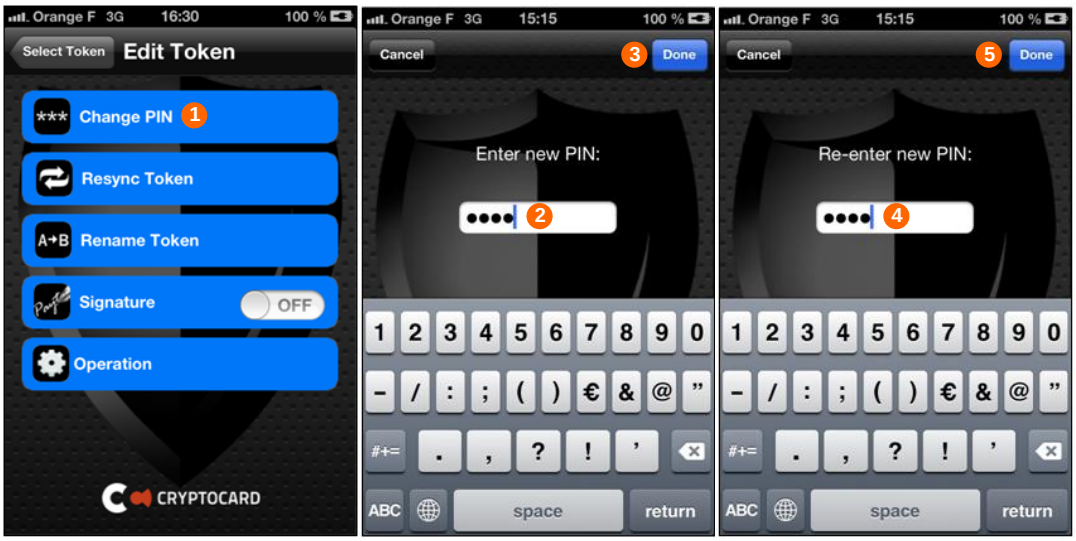

Figure 55: change client-side PIN Code

how do I resynchronize my MP token?

1. **Within the SAS self-service portal:** within the "Home" page tap "Resync Token" 1, within the "User" page enter your user ID in the "User ID" field 2, tap "Next" 3, enter the serial of your MP token in the "Serial" field 4, then tap "Next" 5.

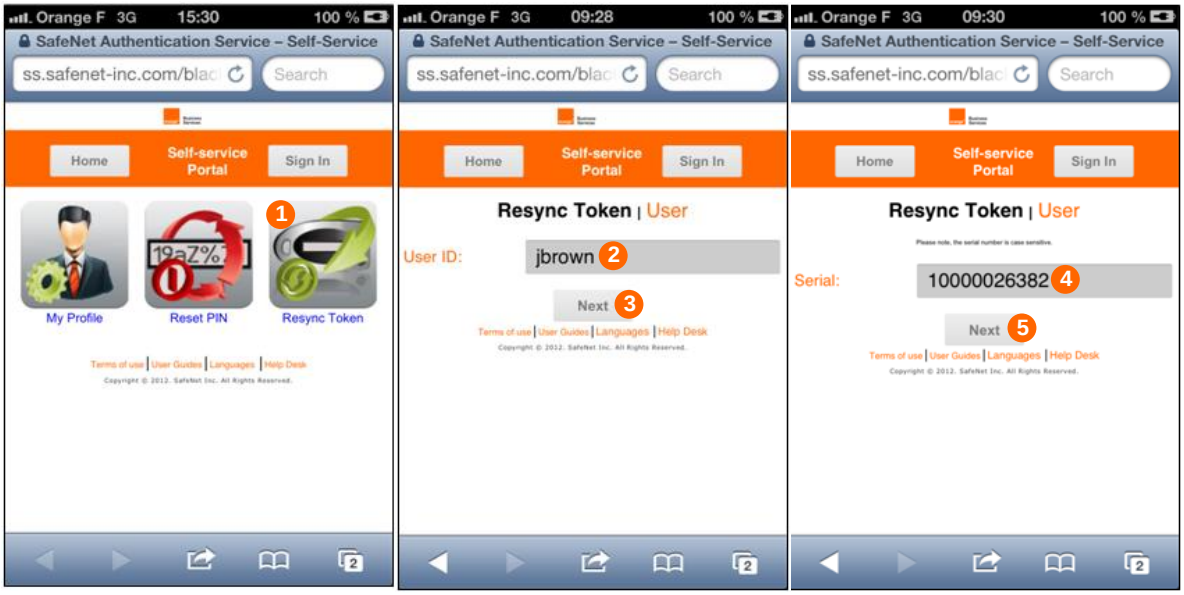

Figure 56: resynchronize token (1/2)

2. **Within the SAS self-service portal:** within the "Challenge/Response" page copy the challenge value ❶ (hold your finger on the value until the "Copy" icon appears).

3. **Within your "MP" application:** within the "Edit Token" screen tap "Resync Token" ❷, within the "Resync Token" screen paste the challenge value in the "Enter Challenge for token" field ❸ (hold your finger on the field until the "Paste" icon appears), tap "Done" ❹, copy the generated response value ❺ (hold your finger on the value until the "Copy" icon appears).

4. **Within the SAS self-service portal:** within the "Challenge/Response" page paste the response value in the "Response" field ❻ (hold your finger on the field until the "Paste" icon appears), then click on "OK" ❼. Within the "Confirmation" page a message indicates your token resynchronization is successful ❽.

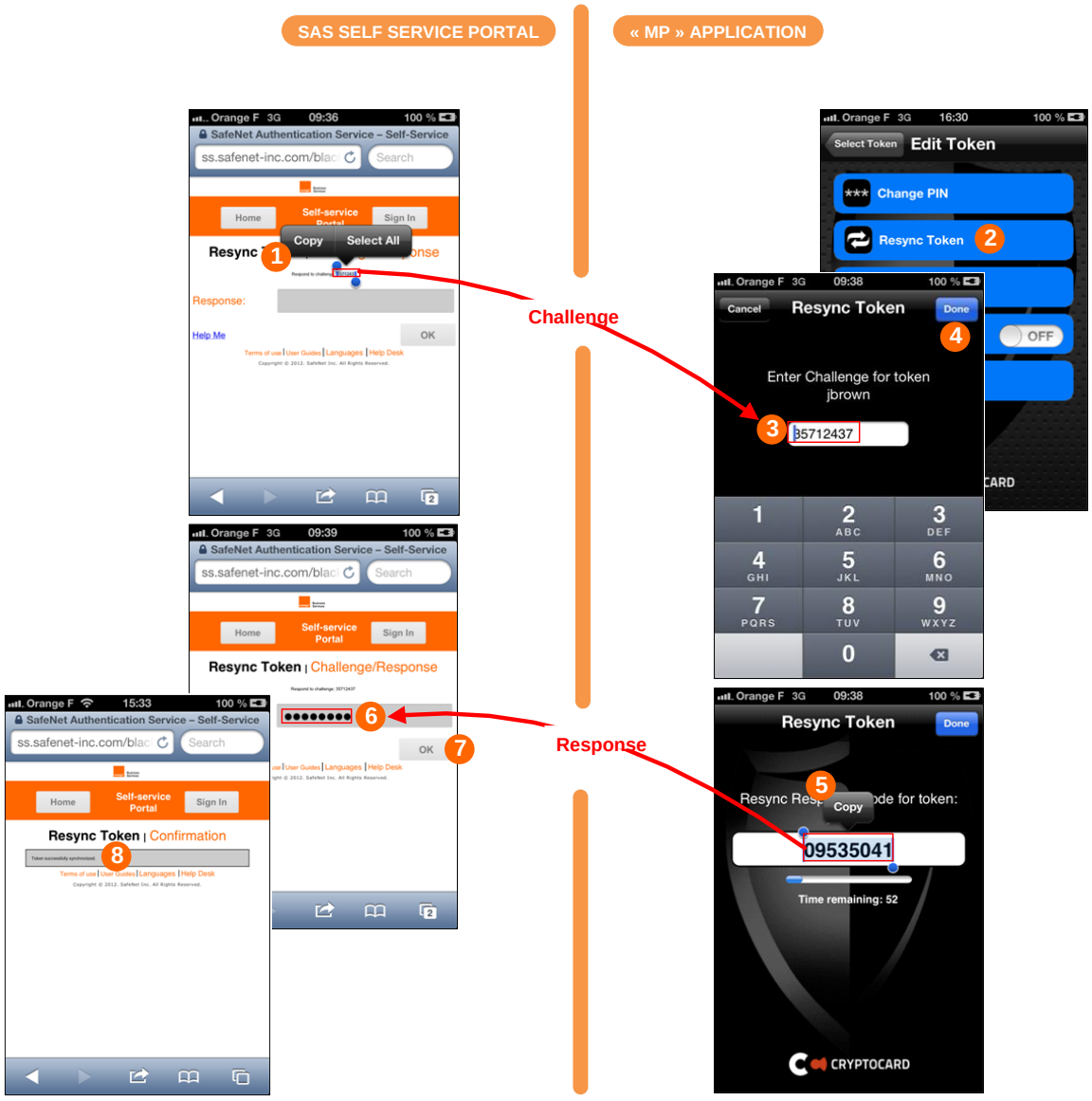

Figure 57: resynchronize token (2/2)

- **"The token cannot be synchronized" error message:** try to resynchronize your MP token again, making sure to copy/paste the right challenge/response values.

how do I rename my MP token?

By default, MP token name is based on your user ID.

Within your "MP" application: within the "Edit Token" screen tap "Rename Token" 1, within the "Rename Token" screen enter the new MP token name in the "Enter New Name" field 2, tap "Done" 3, within "the Edit Token" screen tap "Select Token" 4. Within the "Edit Token" screen, your MP token is now referenced with the new name 5.

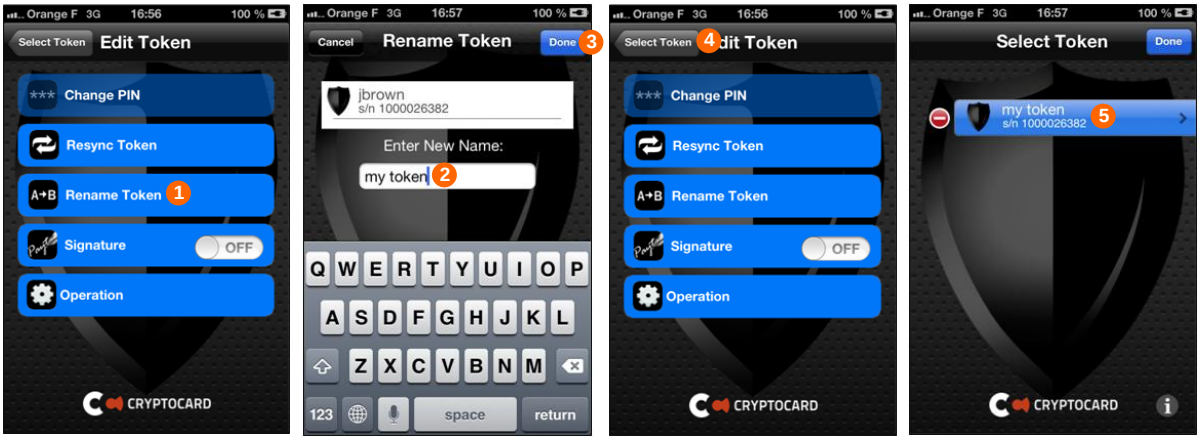

Figure 58: rename token

how do I retrieve my MP token serial?

Within your "MP" application: within the "Edit Token" screen tap "Operation" 1, within the "Operation" memorize the displayed MP token serial 2, then tap "Done" 3 to return to the "Edit Token" screen.

Figure 59: retrieve token serial

how do I remove a MP token?

For maintenance or troubleshooting purposes, your usual help desk may ask you to remove a MP token from your device.

Within your "MP" application: within the "Select Token" screen tap "Edit" ❶, the red symbol to the left of the token ❷, "Delete" ❸, then "Delete Token" ❹.

Figure 60: remove token

how do I retrieve the "MP" application version?

For maintenance or troubleshooting purposes, your usual help desk may ask you the version of your MP application.

Within your "MP" application: within the "Select Token" screen tap the "Information" icon ❶, memorize the displayed "MP" application version ❷, then tap "Done" ❸ to return to the "Select Token" screen.

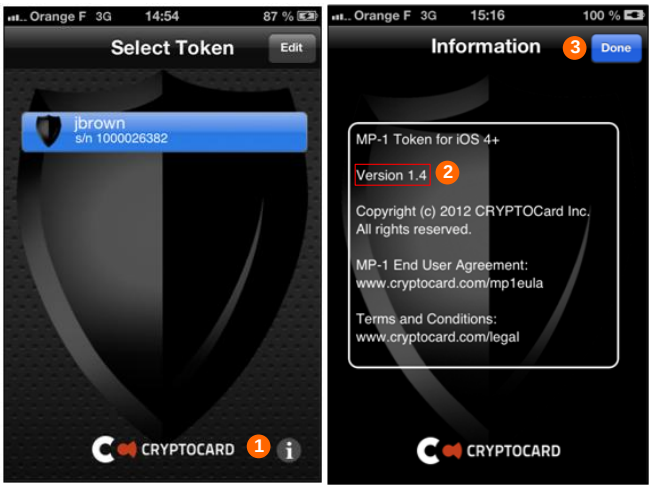

Figure 61: retrieve MP application version

how do I uninstall the “MP” application?

For maintenance or troubleshooting purposes, your usual help desk may ask you to uninstall the “MP” application from your iPhone.

Within your iPhone home screen: hold your finger on the MP application icon until the icon begins to shake or wiggle ❶, tap "x" in the upper left hand corner of the icon ❷, then tap “Delete” within the pop-up window ❸.

Figure 62: uninstall MP application

KT token

Orange Business Services would like to thank you for choosing our Secure Authentication service to help you protect your on-line identity and the networks, applications and data you use from unauthorized access.

In this chapter, you will find instructions for installing, activating and managing your KT token.

what is a KT token?

Up until now, you've logged on with your User Name and Password. The problem is that passwords are easily compromised, putting your identity and the resources you access at risk. By using a KT token, you will be able to generate a "One-time Password" or "OTP". As the name implies, an OTP can only be used once. Each time you logon you will use your KT token to generate a new OTP.

what is a KT token?

The KT-5 Key Chain token generates a new, pseudo-random Token Code each time the token is activated. The KT token is activated by pressing the button located to the right and below the LCD display.

The KT Token Code consists of a string of 8 characters that is used to guard against unauthorized use.

how does it protect me?

Password theft is the single most common way thieves and hackers steal identities and gain unauthorized access to networks and resources. While they have many ways to steal a password, success depends on the stolen password being valid, much the way credit card theft relies on the card being usable until you report it as stolen. The problem of course is that it is almost impossible for you or the security professionals that manage your network to discover your password has been compromised until long after damage has been done.

The KT token solves this problem because the instant you logon with your OTP, it is no longer valid. Any attempt to logon by reusing the OTP will not only fail, but also instantly alert your network security professionals to a possible attack on your identity.

Thanks to PIN Code protection, your KT token is protected against unauthorized use by a PIN Code only you know. Again, much like a bank card or "Chip and PIN" credit card, the thief not only needs access to your KT token but must know your PIN Code as well. Any attempt to use the KT token with and incorrect PIN Code will fail. Successive attempts to guess your PIN Code will automatically "lock" your KT token, effectively disabling it, giving you and your network security professionals time to deal with the threat.

what kind of PIN Code is supported by KT token?

- **Server-side user-selected PIN Code:** the PIN Code is stored and managed at the Secure Authentication server level. You have the ability to change it at any time. Token Codes are generated without entering any PIN Code in the "Token" application (OTP=PIN Code+Token Code).
- **Server-side fixed PIN Code:** the PIN Code is stored and managed at the Secure Authentication server level. The PIN Code displayed during MP token installation is permanent, you can not change it. Token Codes are generated without entering any PIN Code in the "Token" application (OTP=PIN Code+Token Code).

what are my responsibilities?

Using the KT token will not only provides security, it will simplify your life be reducing or eliminating the need to remember or periodically change passwords. Your KT token will do this for you, every time you logon. However, you do have a few simple obligations.

protect your PIN Code

You have to protect your PIN Code just as you would the PIN Code for your bank or credit card. Never share it with anybody, including people you trust. Your usual help desk will never ask for your PIN Code and you should never reveal it to them. Never write down your PIN Code.

what if I forget my PIN Code?

Contact your usual help desk. Upon verifying your identity they will be able to reset your PIN Code.

what if my KT token is locked?

Contact your usual help desk. Upon verifying your identity they will be able to unlock your KT token.

how long will my KT token continue to operate?

Your KT token will be able to generate OTPs until it is revoked by IT administrators.

what should I do if I can't logon using my token?

The most common cause of failed logon is entering an incorrect OTP. Never attempt to reuse a Token Code and ensure that you enter the Token Code exactly as displayed on the token, including any upper and lower case letters and punctuation that it may contain.

By default, your account will automatically lock for 15 minutes if more than 3 consecutive logon attempts fail. You must wait this amount of time before your account will unlock. Contact your usual help desk to resolve logon problems.

how do I enroll with a KT token?

Within your e-mail client: open the "SAS Self-enrollment" message 1, and click on the self-enrollment URL link 2: your web browser will connect to the Secure Authentication enrollment web site.

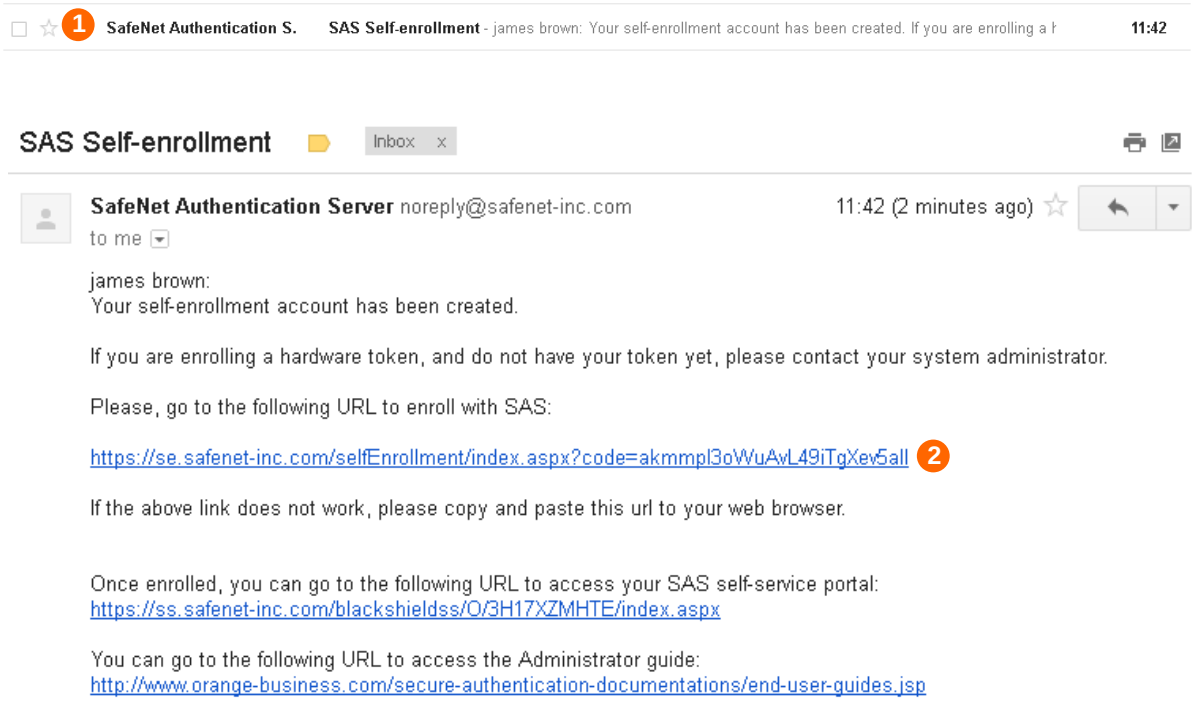

Figure 63: self-enrollment link

- **"SAS Self-enrollment" e-mail not received:** verify if the mail is not stored in the "junk" folder of your e-mail client.
- **"Your provisioning task has already been completed" error message:** verify you opened the latest self-enrollment message, and not an old one.

how do I register my KT token?

1. **With your KT token:** memorize the serial number on the back of your token ❶.
2. **Within your web browser:** enter the serial number value in the "Serial Number" field ❷ and click on "Next" ❸.

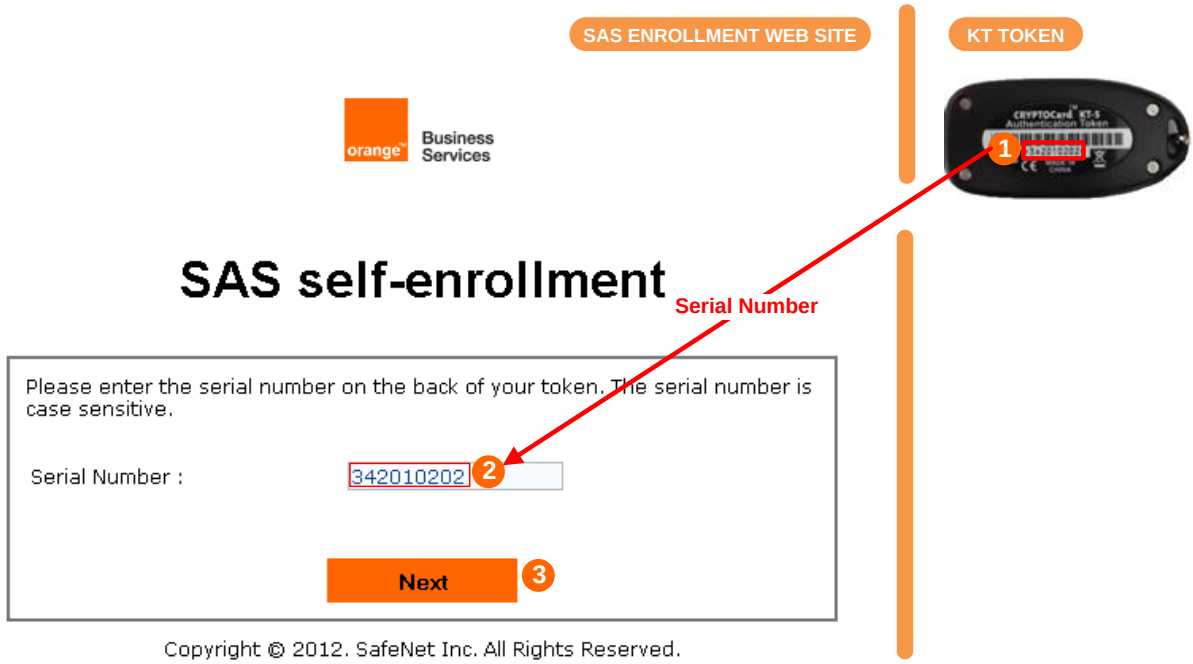

Figure 64: register token serial

- **"There is no token matching the serial number provided" error message :** close your browser, click the self-enrollment URL link again, register your KT token again making sure the serial number you enter is correct.

how do I activate my KT token?

1. **Within your web browser:** memorize the displayed PIN Code ❶ (it might be a fixed one, and you have not the ability to know its type at this enrollment step), copy it and paste it in the "OTP" field ❷.

2. **With your KT token:** press button ❸ to both power on the token and generate a new Token Code, then memorize the displayed Token Code ❹.

3. **Within your web browser:** enter the Token Code next to the PIN Code in the "OTP" field ❺ then click on "Next" ❻.

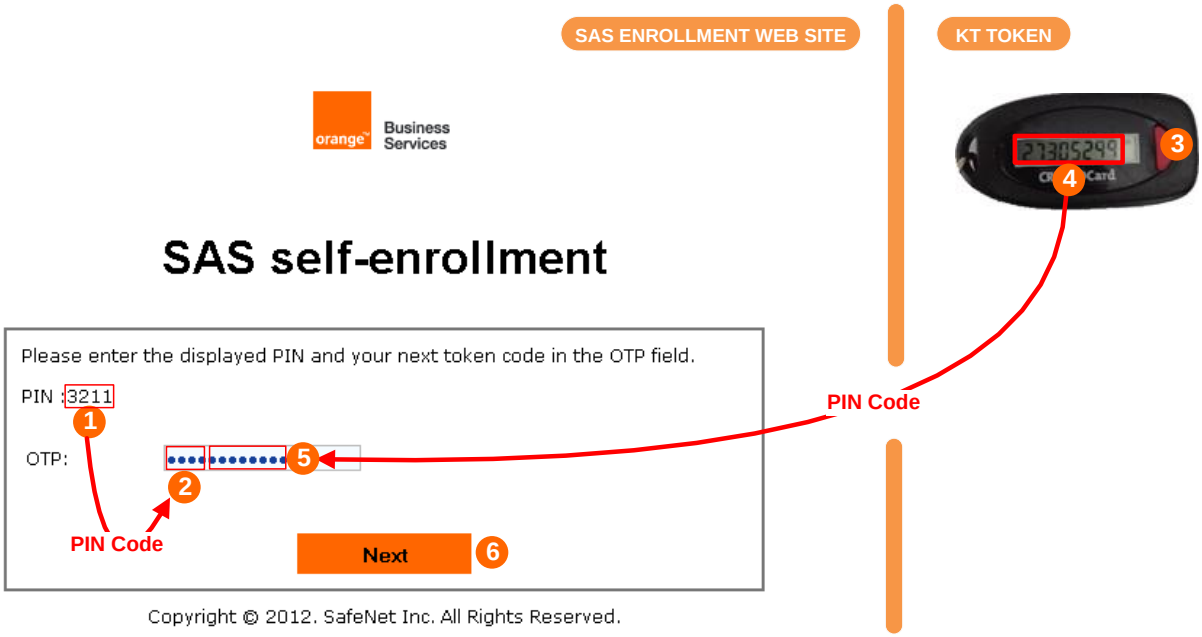

Figure 65: activate token with PIN Code

- **"Authentication failed, enter your OTP again" error message:** if your KT token is still on, press and hold the button (approximately 3-4 seconds) on the token until the "-OFF-" prompt appears, then release the button. Press button to power on the token again and generate a new Token Code.

- **"You have failed to provide the correct response too many times" error message:** contact your usual help desk.

The end of the process depends on the type of the KT token PIN Code.

how do I complete installation process with user-selected PIN code?

Within your web browser: choose your PIN Code, enter it in the "New PIN" and "Verify PIN" fields ❶ then click on "Next" ❷. The enrollment web site displays a page that confirms your MP token has been successfully activated. Memorize your User ID ❸, then click on "Close" ❹ (when using Firefox you have to close the browser).

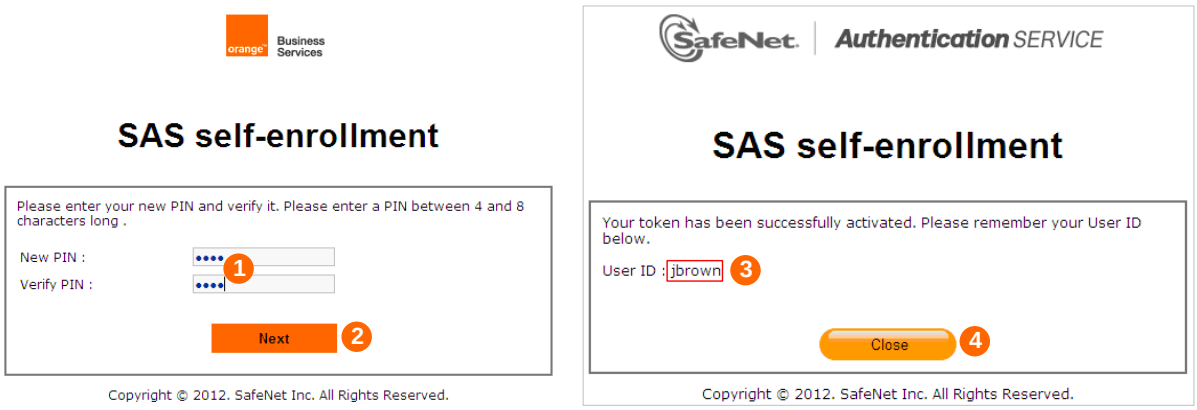

Figure 66: activate token with user selected PIN

- **"PIN change failed" error message:** try to enter your new PIN Code again making sure to meet complexity requirements displayed.
- **"You have failed to provide the correct response too many times" error message:** contact your usual help desk.

how do I complete installation process with fixed PIN code?

Within your web browser: the enrollment web site displays a page that confirms your MP token has been successfully activated. Memorize your User ID ❶, then click on "Close" ❷ (when using Firefox you have to close the browser).

Figure 67: activate token with user selected PIN

how do I authenticate with my KT token?

You have the ability to test authentication with your MP token thanks to the SAS self-service portal.

1. **Within your e-mail client:** open the “SAS Self-enrollment” message 1 again, and click on the SAS self-service portal URL link 2: your web browser will connect to the self-service web site.

2. **Within the SAS self-service portal:** within the “Home” page click on “Sign In” 3, within the “Authenticate” page click on “Sign in using your token” 4.

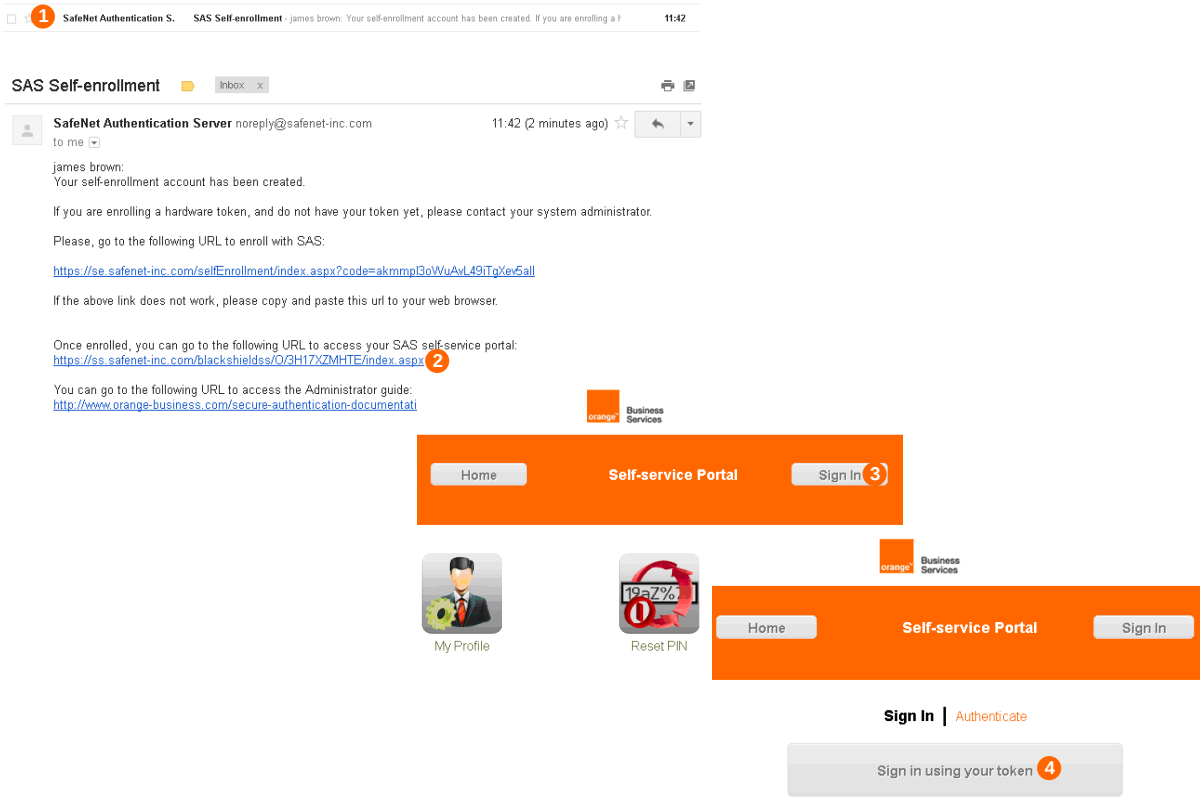

Figure 68: access to the SAS self-service portal sign in page

3. **Within the SAS self-service portal:** within the "Authenticate to Process" page enter your user ID in the "User ID" field ❶ and your PIN Code in the "OTP" field ❷.

4. **With your KT token:** press button ❸ to both power on the token and generate a new Token Code, then memorize the displayed Token Code ❹.

5. **Within the SAS self-service portal:** within the "Authenticate to Process" page paste the Token Code value next to the PIN Code in the "OTP" field ❺, then click on "OK" ❻. The "Sign Out" button ❼ displayed within the "Home" page indicates your authentication is successful.

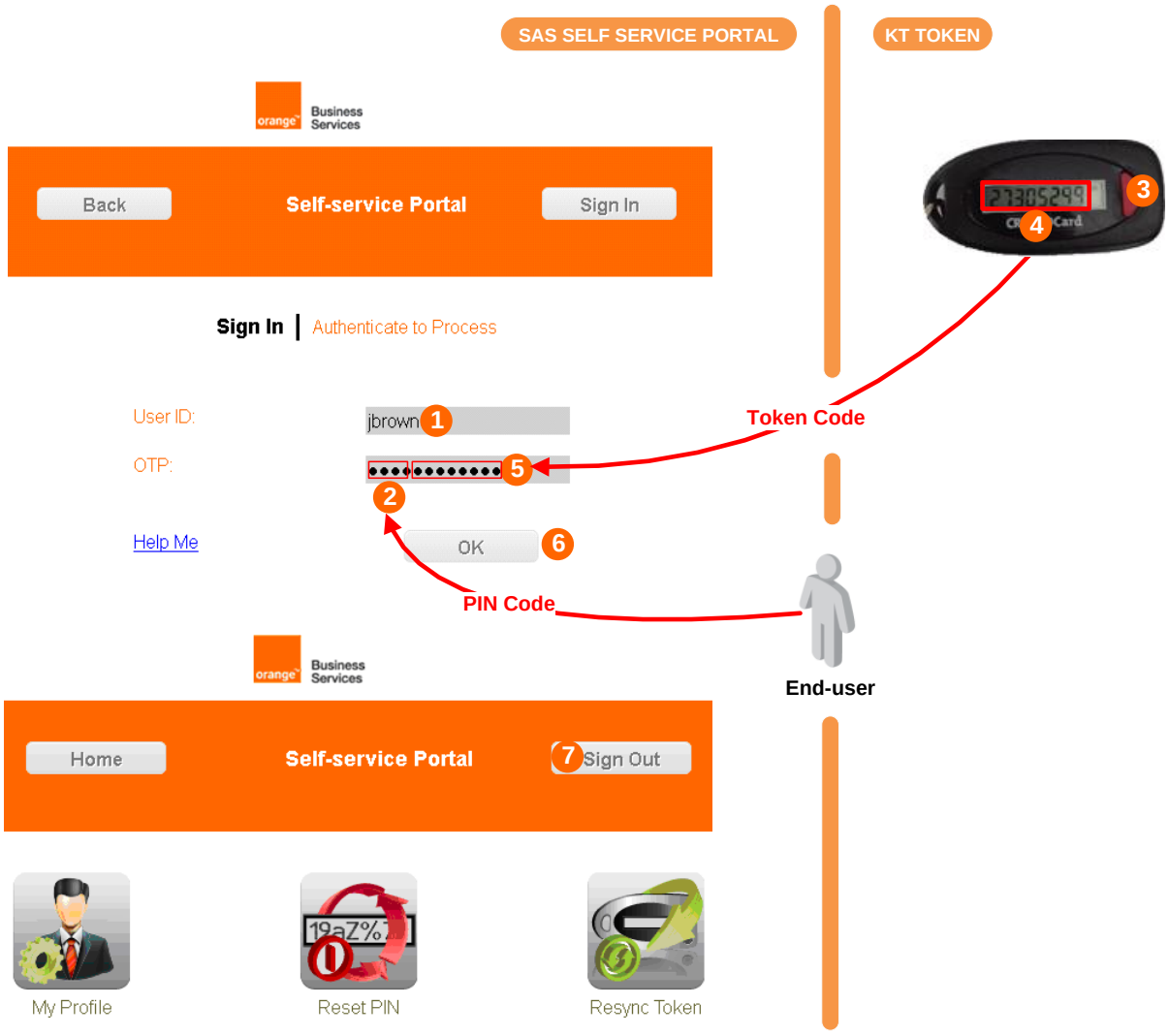

Figure 69: authenticate

- **"Authentication failed, enter your OTP again" error message:** if your KT token is still on, press and hold the button (approximately 3-4 seconds) on the token until the "-OFF-" prompt appears, then release the button. Press button to power on the token again and generate a new Token Code.

how do I change my PIN Code?

Within the SAS self-service portal: within the "Home" page, once authenticated ("Sign Out" button must be displayed 1), click on "Reset PIN" 2, within the "Create New PIN" page choose a new PIN Code and enter it in the "Create New PIN" and "Verify PIN" fields 3, then click on "OK" 4. Within the "Create New PIN" page a message indicates your PIN Code change is successful 5.

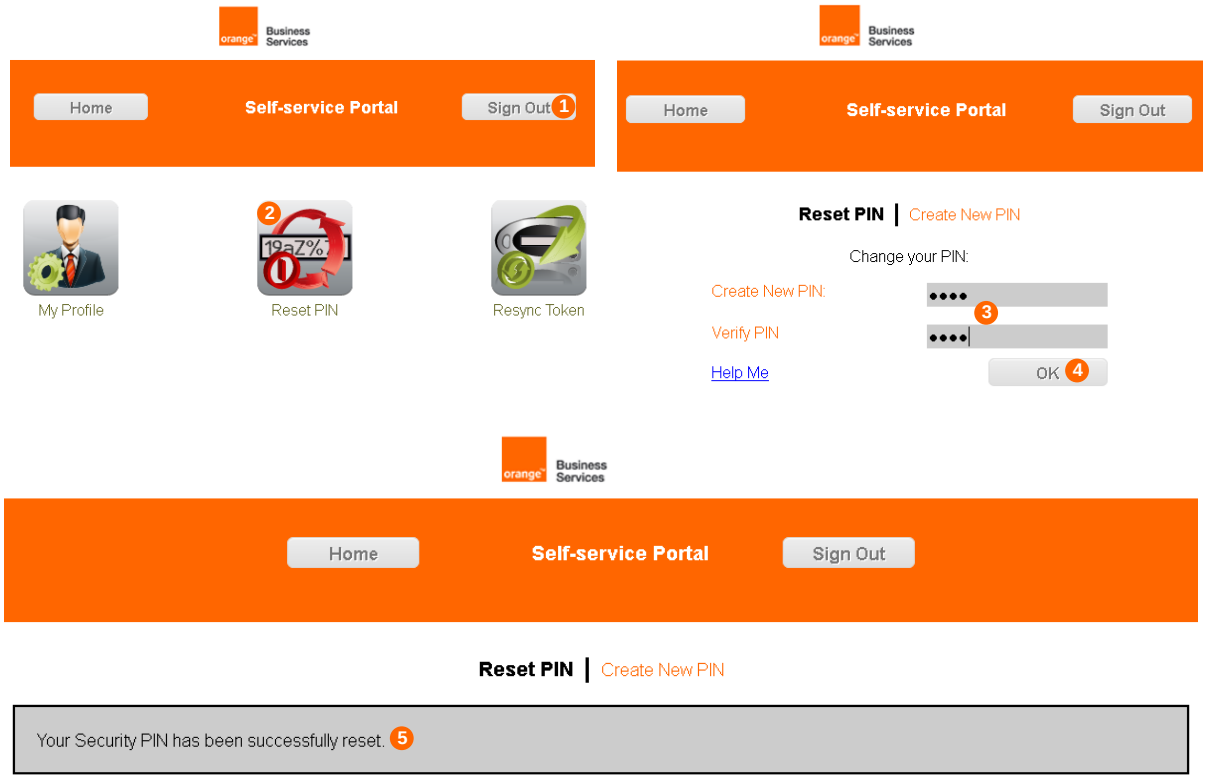

Figure 70: change PIN Code

- **If the self-service portal displays the "PIN does not meet complexity requirements." Message:** Try to enter a new PIN again making sure to meet complexity requirements displayed.
- **If the self-service portal displays the "No tokens are enabled to change the Personal Identification Number (PIN)" message:** Your KT token has a server fixed PIN Code, you can't change it.

how do I resynchronize my KT token?

1. **Within your web browser:** within the “Home” page click on “Resync Token” 1, within the “User” page enter your user ID in the “User ID” field 2, click on “Next” 3.
2. **With your KT token:** memorize the serial number on the back of your token 4.
3. **Within your web browser:** enter the serial number value in the “Serial” field 5 then click on “Next” 6.

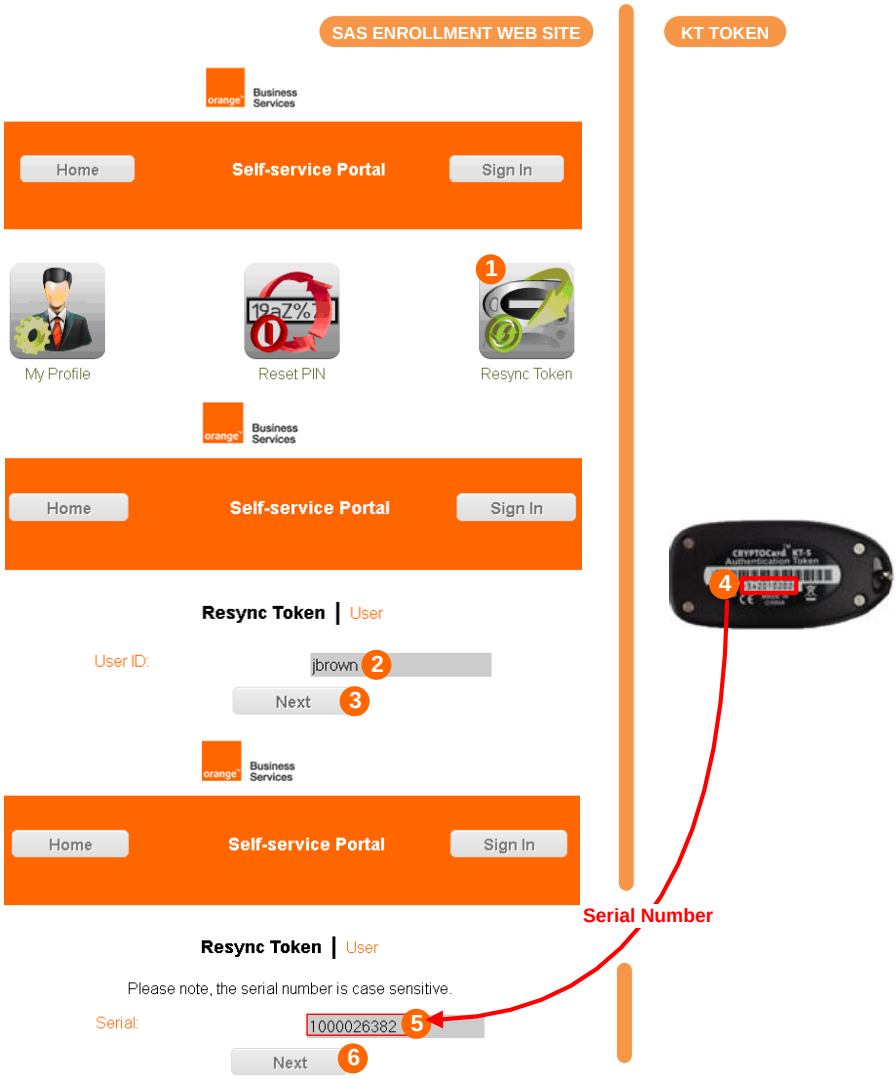

Figure 71: resynchronize token (1/2)

Resynchronization requires you to enter a “challenge” within your KT token.

4. **Within the SAS self-service portal:** within the “Challenge/Response” page memorize the “Respond to challenge” value 1.

5. **With your KT token:** press button ❷ power on the token, then use the button ❸ to choose and validate the digits of the "Respond to challenge" value:

   - press and hold the button (approximately 3-4 seconds) on the token until the **"Init"** prompt appears, then release the button.
   - the token will cycle through a series of prompts: press the button while the **"rESYNC"** prompt is displayed.
   - The digits will be displayed sequentially. For every digit of the resynchronization challenge, press the button to accept the displayed digit.
   - After the last digit of the challenge is displayed, double-press the button.

   Memorize the response value displayed by your token ❹.

6. **Within the SAS self-service portal:** within the "Challenge/Response" page enter the response value in the "Response" field ❺, then click on "OK" ❻. Within the "Confirmation" page a message indicates your token resynchronization is successful ❼.

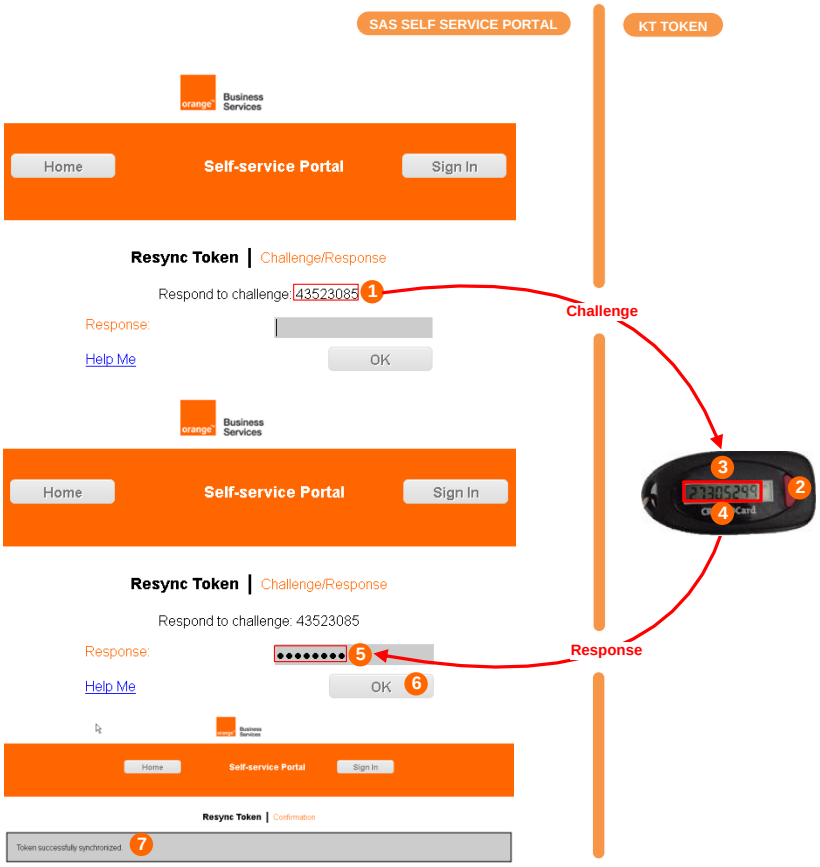

Figure 72: resynchronize token (2/2)

- **"The token cannot be synchronized" error message:** try to resynchronize your MP token again, making sure to copy/paste the right challenge/response values.

GrIDsure token

In this chapter, you will find instructions for activating and managing your GrIDsure token.

what is a GrIDsure token?

GrIDsure is a way of providing an end-user the ability to generate a one-time password, without requiring the end-user to have any additional hardware or software applications. GrIDsure presents the end-user with a grid of cells containing random characters, from which the end-user selects their 'personal identification pattern' (PIP). Each time the end-user needs to authenticate the grid will display a random / unique set of characters. The end-user then just needs to remember their PIP and provide the specific characters within those cells that make up their PIP in order to securely authenticate to the protected network resource.

Up until now, you've logged on with your User Name and Password. The problem is that passwords are easily compromised, putting your identity and the resources you access at risk. By using a MP token, you will be able to generate a "One-time Password" or "OTP". As the name implies, an OTP can only be used once. Each time you logon you will use your MP to generate a new OTP.

how does it protect me?

Password theft is the single most common way thieves and hackers steal identities and gain unauthorized access to networks and resources. While they have many ways to steal a password, success depends on the stolen password being valid, much the way credit card theft relies on the card being usable until you report it as stolen. The problem of course is that it is almost impossible for you or the security professionals that manage your network to discover your password has been compromised until long after damage has been done.

GrIDsure displays a grid of cells containing random characters to an end-user. As shapes and patterns are remembered more simply than words and numbers, GrIDsure involves the end-user to remember a sequence of cells in a pattern on the grid that is easily recognizable to them.

The end-user chooses their "Personal Identification Pattern" (PIP) from the arrangement and sequence of the cells from the grid:

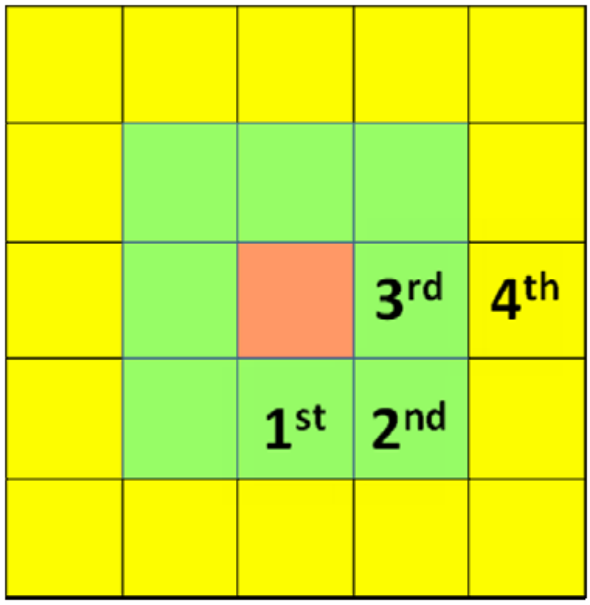

Figure 73: how does it work 1/4

When the end-user is required to authenticate securely to a protected network resource, they select the characters that match their PIP from the unique characters shown to them by the grid.

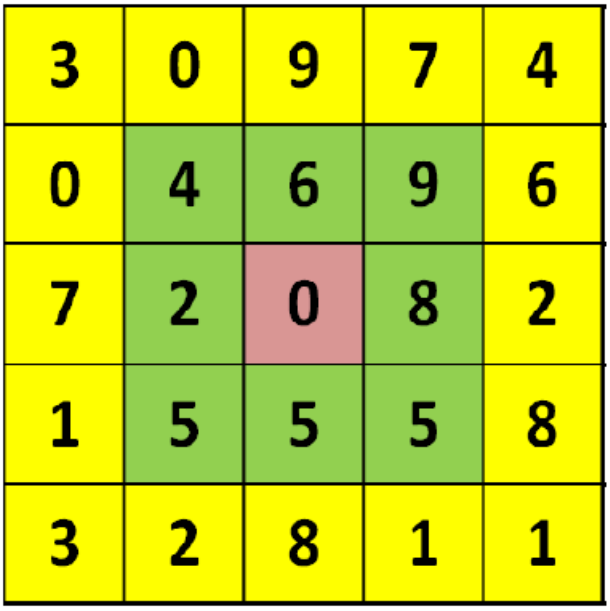

Figure 74: how does it work 2/4

In this example, the end-user's PIP would be a value of: 5582. This is seen in the highlighted cells below. Therefore to authenticate, the end-user would enter 5582 as their one-time password value. The next time the end-user needs to authenticate, the characters displayed by the grid will be different, but the PIP remains the same. The end-user just needs to enter the new characters in their PIP displayed by the grid.

Figure 75: how does it work 3/4

In this example, the end-user would now enter 0182 as their one-time password to authenticate.

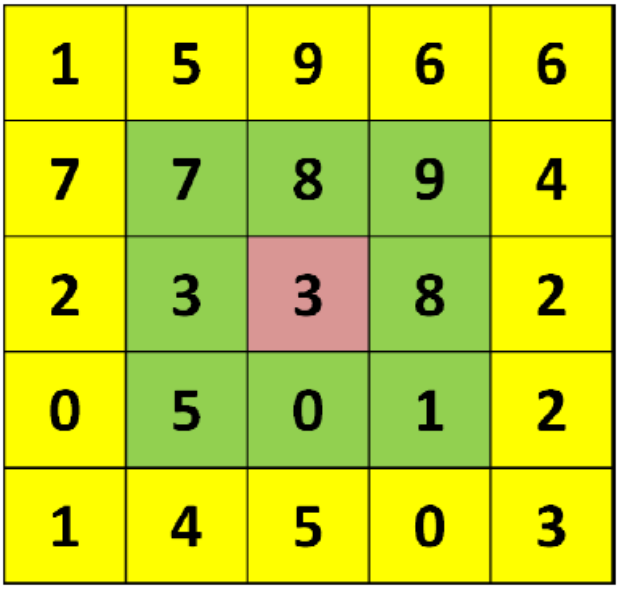

Figure 76: how does it work 4/4

can anybody use my GrIDsure token?

Thanks to PIN Code protection, your GrIDsure token is protected against unauthorized use by a PIN Code only you know. Again, much like a bank card or “Chip and PIN” credit card, the thief not only needs access to your GrIDsure token but must know your PIN Code as well. Any attempt to use the GrIDsure token with and incorrect PIN Code will fail. Successive attempts to guess your PIN Code will automatically “lock” your GrIDsure token, effectively disabling it, giving you and your network security professionals time to deal with the threat.

what kind of PIN Code is supported by GrIDsure token?

- **Server-side user-selected PIN Code:** the PIN Code is stored and managed at the Secure Authentication server level. You have the ability to change it at any time..
- **Server-side fixed PIN Code:** the PIN Code is stored and managed at the Secure Authentication server level. The PIN Code displayed during MP token installation is permanent, you can not change it.

what are my responsibilities?

Using the GrIDsure token will not only provides security, it will simplify your life be reducing or eliminating the need to remember or periodically change passwords. Your GrIDsure token will do this for you, every time you logon. However, you do have a few simple obligations.

protect your PIN Code

You have to protect your PIN Code just as you would the PIN Code for your bank or credit card. Never share it with anybody, including people you trust. Your usual help desk will never ask for your PIN Code and you should never reveal it to them. Never write down your PIN Code.

what if I forget my PIN Code?

Contact your usual help desk. Upon verifying your identity they will be able to reset your PIN Code.

what if my GrIDsure token is locked?

Contact your usual help desk. Upon verifying your identity they will be able to unlock your GrIDsure token.

how long will my GrIDsure token continue to operate?

Your GrIDsure token will be able to generate OTPs until it is revoked by IT administrators.

what should I do if I can't logon using my token?

The most common cause of failed logon is entering an incorrect OTP. Never attempt to reuse a Token Code and ensure that you enter the Token Code exactly as displayed on the token, including any upper and lower case letters and punctuation that it may contain.

By default, your account will automatically lock for 15 minutes if more than 3 consecutive logon attempts fail. You must wait this amount of time before your account will unlock. Contact your usual help desk to resolve logon problems.

how do I enroll with a GrIDsure token?

how do I access the enrollment web site?

Within your e-mail client: open the "SAS Self-enrollment" message 1, and click on the self-enrollment URL link 2: your web browser will connect to the Secure Authentication enrollment web site.

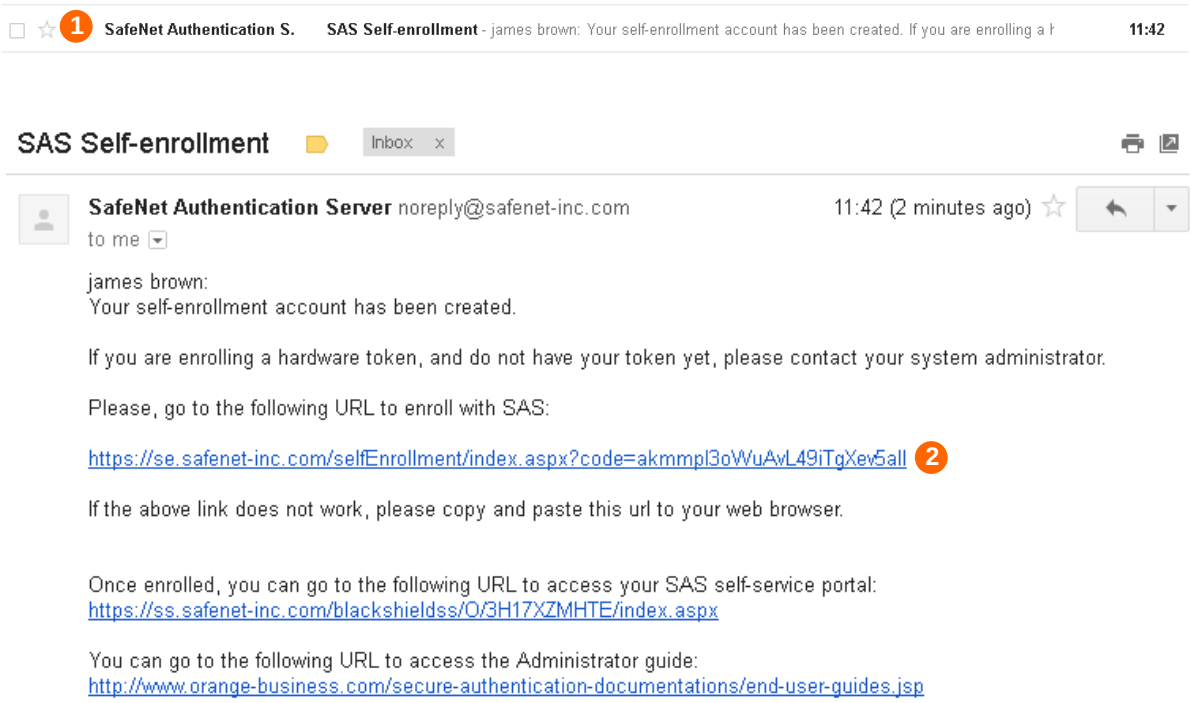

Figure 77: self-enrollment link

how do I create my PIP?

Within your web browser: select your PIP using the grid. Try to pick a pattern (here a b c d) that would be not easily guessed by someone else. Memorize the displayed PIN Code 2 (this might be your definitive one if the type of the PIN Code is fixed), then click on "Next" 3. The enrollment web site displays a page that confirms your MP token has been successfully activated. Memorize your User ID 4, then click on "Close" 5 (when using Firefox, you have to close the browser).

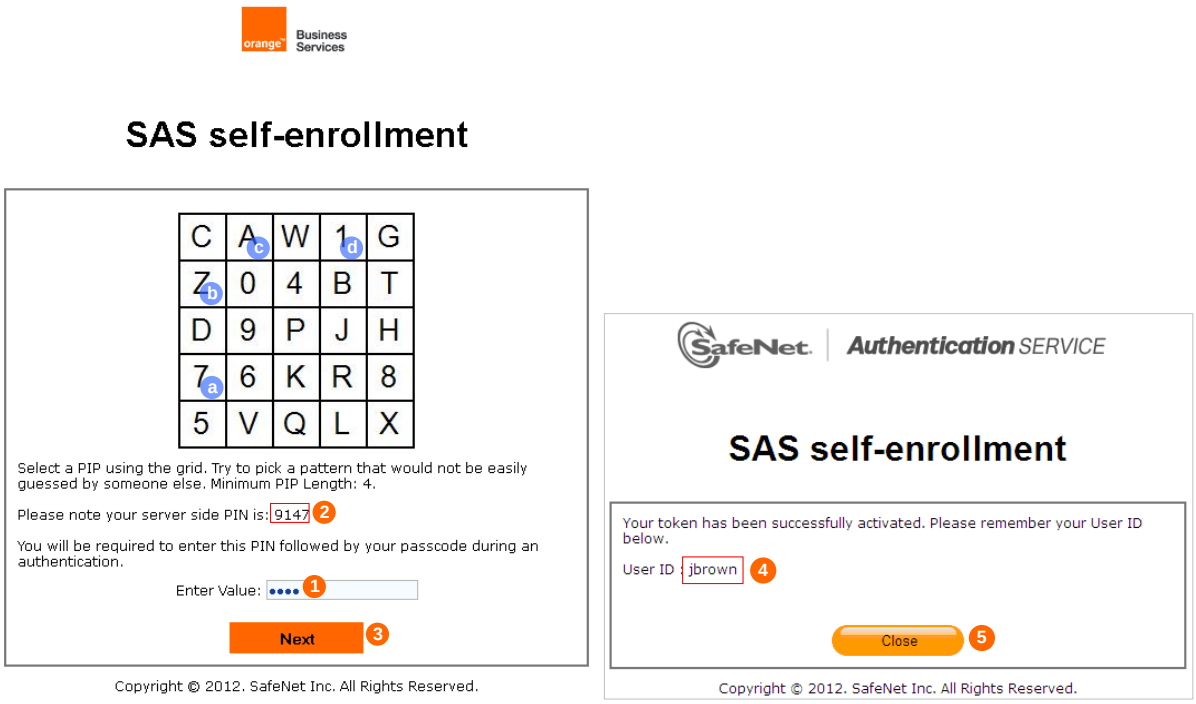

Figure 78: create PIP

- **If the enrollment web site displays the "PIP change failed" message:**
  Try to enter your new PIP again making sure to meet complexity requirements displayed.

- **If the enrollment web site displays the "You have failed to provide the correct response too many times" message:**
  Contact your usual help desk.

Select your PIP using the grid. Try to pick a pattern (here a b c d) that would be not easily guessed by someone else. Enter the values corresponding to your pattern (here "RVZ2") in the "Enter Value" field 1 then click on "Next" 2. The enrollment web site displays the last page that confirms your GrIDsure token has been enabled. Memorize your User ID before clicking on "Close" (when using Firefox, the "Close" button do not exist, you have to close your browser instead).

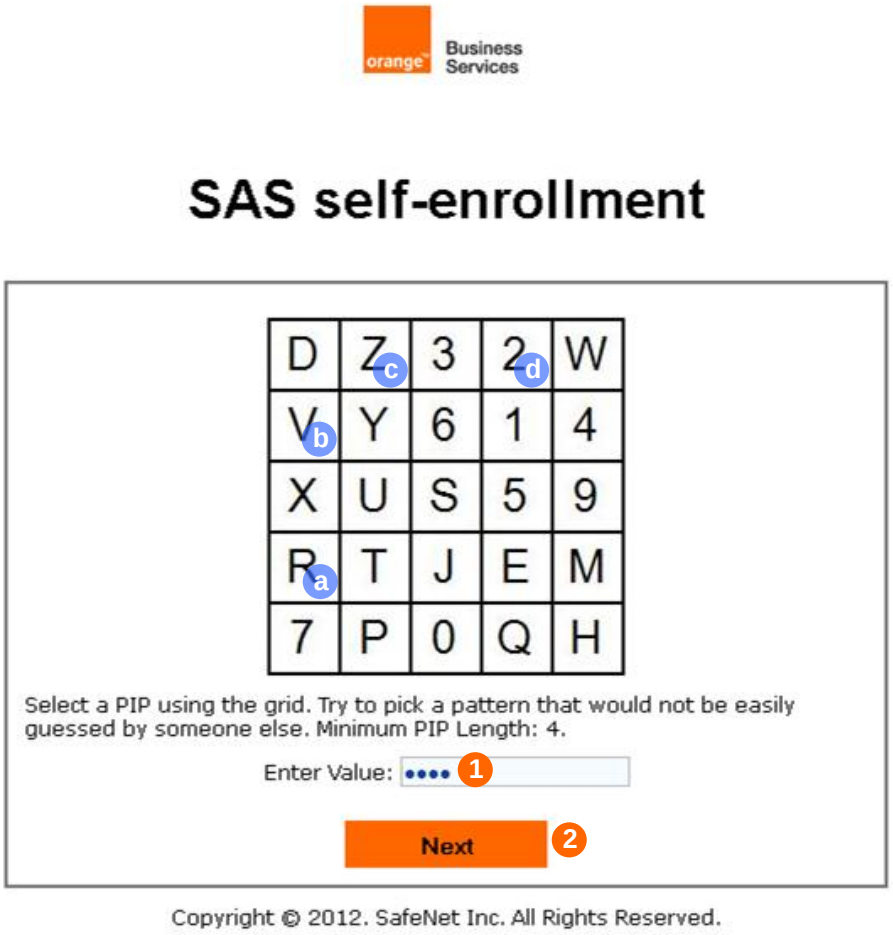

Figure 79: create PIP

- **"PIP change failed" error message:** try to enter your new PIP again making sure to meet complexity requirements displayed.
- **"You have failed to provide the correct response too many times" error message:** contact your usual help desk.

how do I authenticate with my GrIDsure token?

You have the ability to test authentication with your GrIDsure token thanks to the SAS self-service portal.

1. **Within your e-mail client:** open the “SAS Self-enrollment” message 1 again, and click on the SAS self-service portal URL link 2: your web browser will connect to the self-service web site.

2. **Within the SAS self-service portal:** within the “Home” page click on “Sign In” 3, within the “Authenticate” page click on “Sign in using your token” 4.

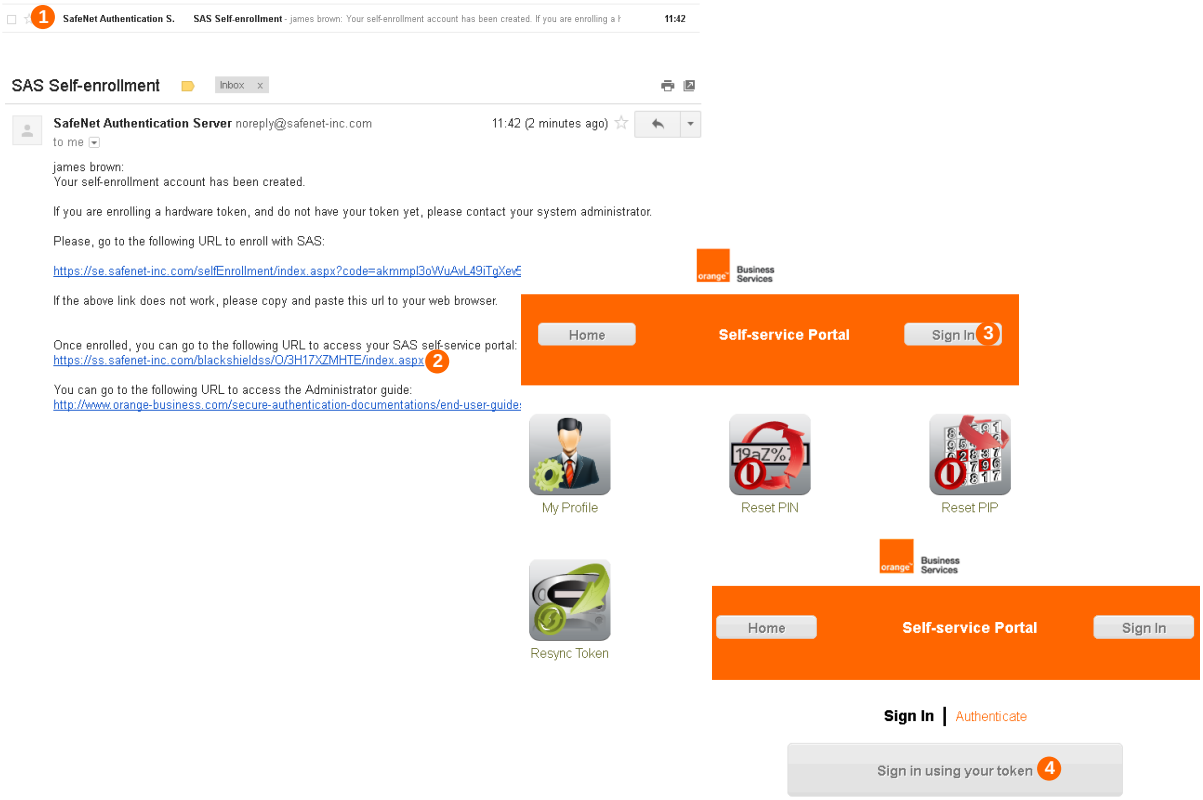

Figure 80: access to the SAS self-service portal sign in page

3. **Within the SAS self-service portal:** within the "Authenticate to Process" page enter your User ID in the "User ID" field ❶, *leave the "OTP" field empty* ❷, click on "OK / Get Grid" ❸, enter your PIN Code in the "OTP" field ❹, enter the values corresponding to your pattern ⓐ ⓑ ⓒ ⓓ (here "8675") next to the PIN Code in the "OTP" field ❺ then click on "OK" ❻. The "Sign Out" button ❼ displayed within the "Home" page indicates your authentication is successful.

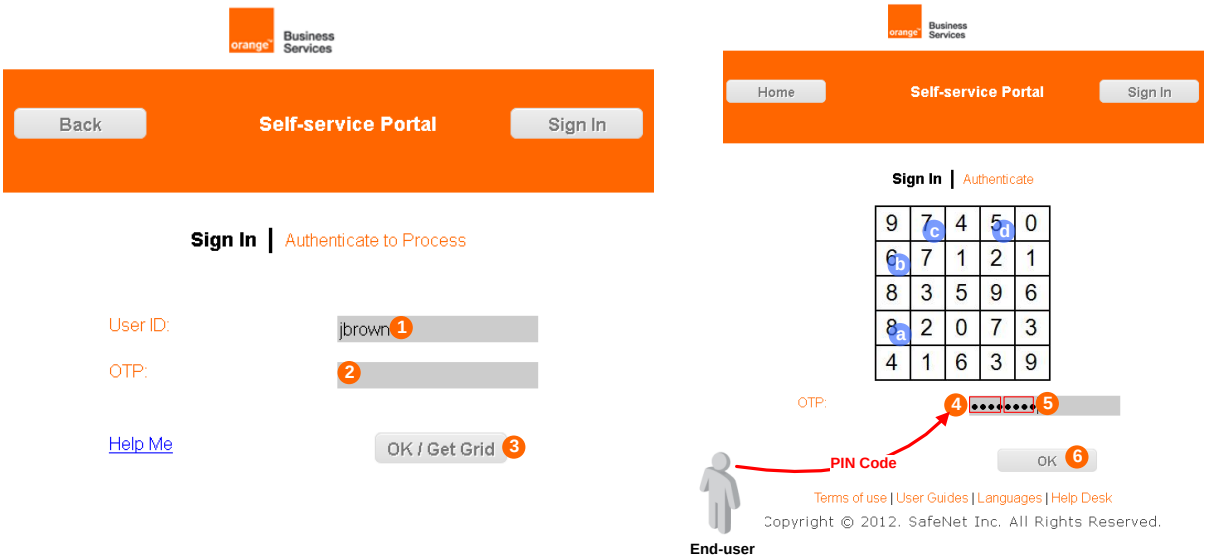

Figure 81: authenticate (common part)

- **"Your login attempt was not successful" error message:** try to authenticate again, making sure to enter your PIN Code followed by the Token Code generated by your MP token in the "OTP" field.

The end of the authentication process depends on the type of the GrIDsure token PIN Code.

user-selected PIN Code

Within the SAS self-service portal: within the “Authenticate” page choose a new PIN Code and enter it in the “New PIN” and “Confirm New PIN” fields 1, then click on “OK” 2. The “Sign Out” button 3 displayed within the “Home” page indicates your authentication is successful.

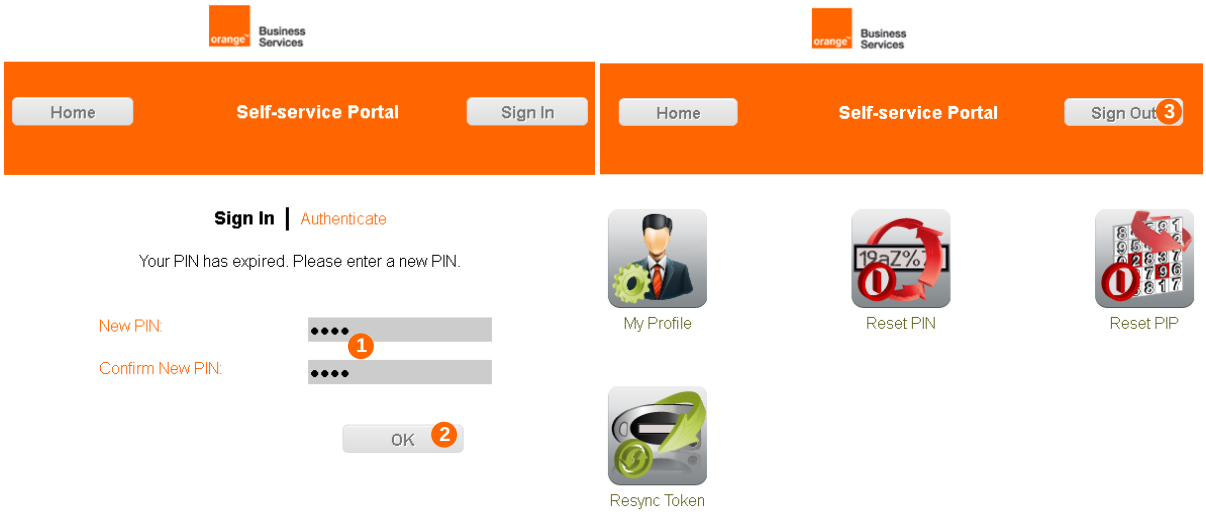

Figure 82: authenticate (with server-side PIN Code)

fixed PIN Code

Within the SAS self-service portal: the “Sign Out” button 1 displayed within the “Home” page indicates your authentication is successful.

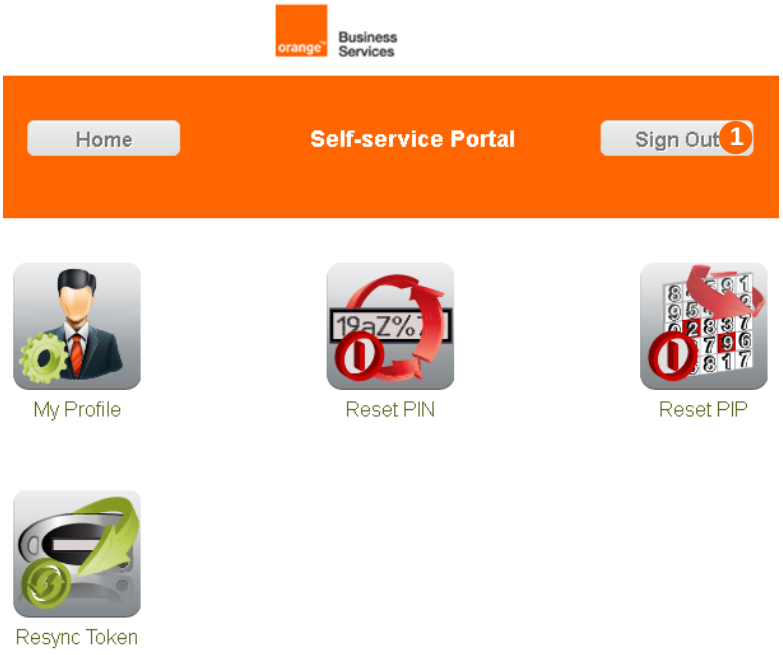

Figure 83: authenticate (with fixed PIN Code)

how do I change my PIN Code?

Within the SAS self-service portal: within the “Home” page, once authenticated (“Sign Out” button must be displayed 1), click on “Reset PIN” 2, within the “Create New PIN” page choose a new PIN Code and enter it in the “Create New PIN” and “Verify PIN” fields 3, then click on “OK” 4. Within the “Create New PIN” page a message indicates your PIN Code change is successful 5.

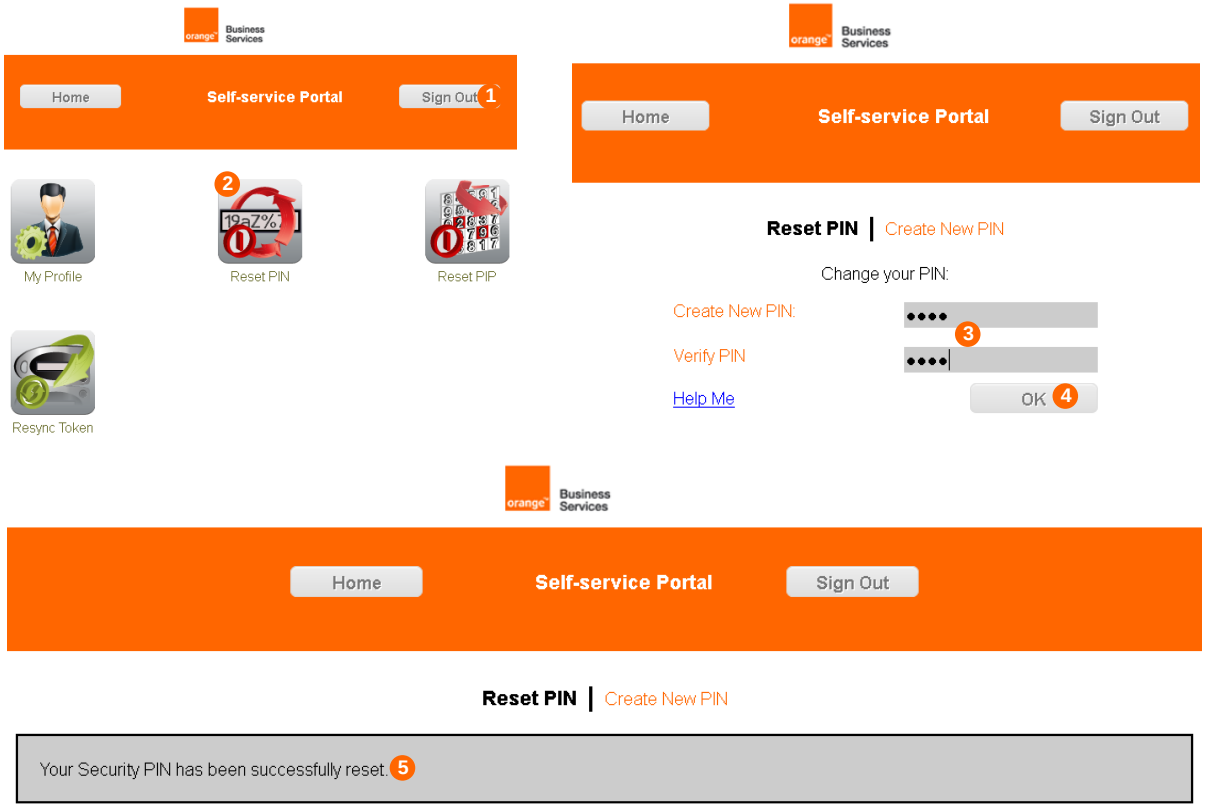

Figure 84: change PIN Code

how do I change the PIP of my GrIDsure token?

Within the SAS self-service portal: once authenticated ("Sign Out" button must be displayed 1) click on "Reset PIP" 2, within the "Select Pattern" page enter the values corresponding to your new pattern a b c d (here "DWH7") in the "Enter cell values" field 3 then click on "OK" 4.

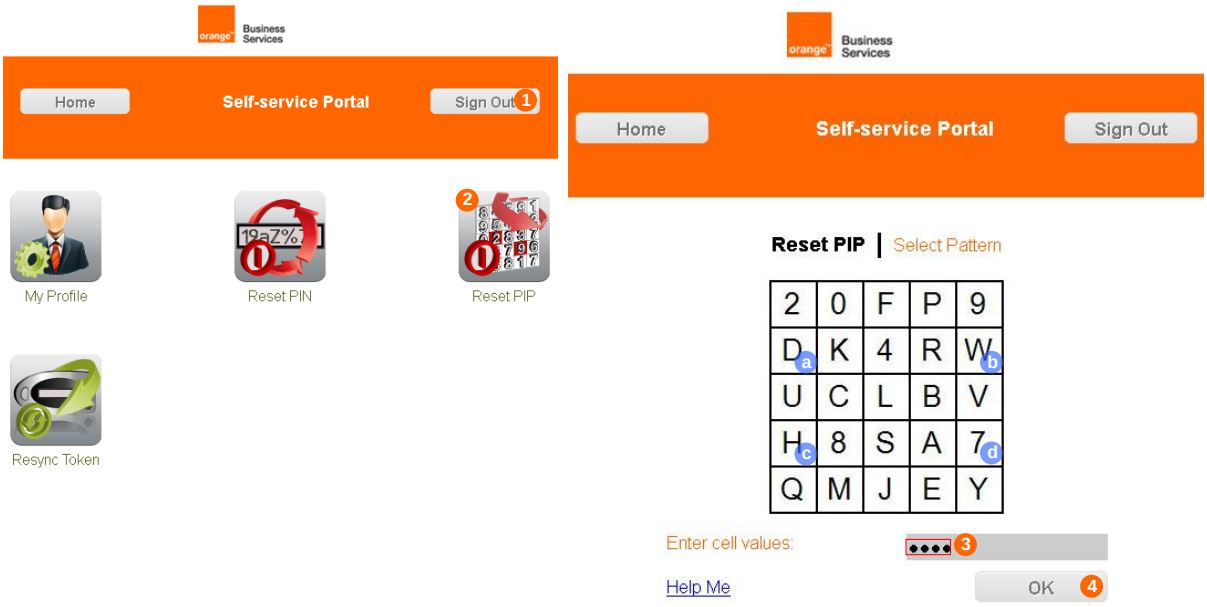

Figure 85: change token PIP

Password

In this chapter, you will find instructions for activating and managing your password.

what is a password?

Single-factor authentication (SFA) is the traditional security process that requires a user name and password before granting access to the user.

what are my responsibilities?

You do have a few simple obligations.

protect your password

You have to protect your password just as you would the PIN Code for your bank or credit card. Never share it with anybody, including people you trust. Your usual help desk will never ask for your password and you should never reveal it to them.

what if my password token is locked?

Contact your usual help desk.

how long will my password continue to operate?

Your password will continue to operate until it is revoked by IT administrators.

what should I do if I can't logon using my token?

The most common cause of failed logon is entering an incorrect password. By default, your account will automatically lock for 15 minutes if more than 3 consecutive logon attempts fail. You must wait this amount of time before your account will unlock. Contact your usual help desk to resolve logon problems.

how do I enroll with a password?

how do I access the enrollment web site?

Within your e-mail client: open the "SAS Self-enrollment" message 1, and click on the self-enrollment URL link 2: your web browser will connect to the Secure Authentication enrollment web site.

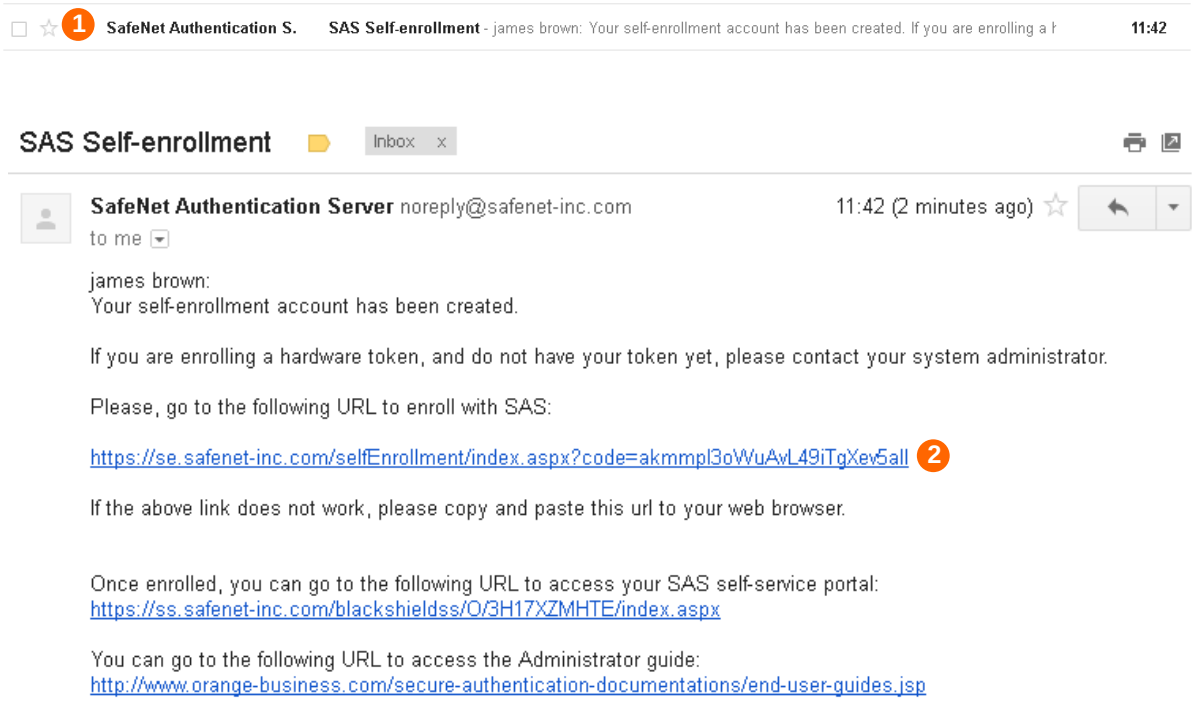

Figure 86: self-enrollment link

- **"SAS Self-enrollment" e-mail not received:** verify if the mail is not stored in the "junk" folder of your e-mail client.
- **"Your provisioning task has already been completed" error message:** verify you opened the latest self-enrollment message, and not an old one.

how do I create my password?

Within your web browser: choose your password and enter it in the "Enter Password" and "Confirm Password" fields ❶ then click on "Next" ❷. The enrollment web site displays a page that confirms your password has been successfully activated. Memorize your User ID ❸, then click on "Close" ❹ (when using Firefox, you have to close the browser).

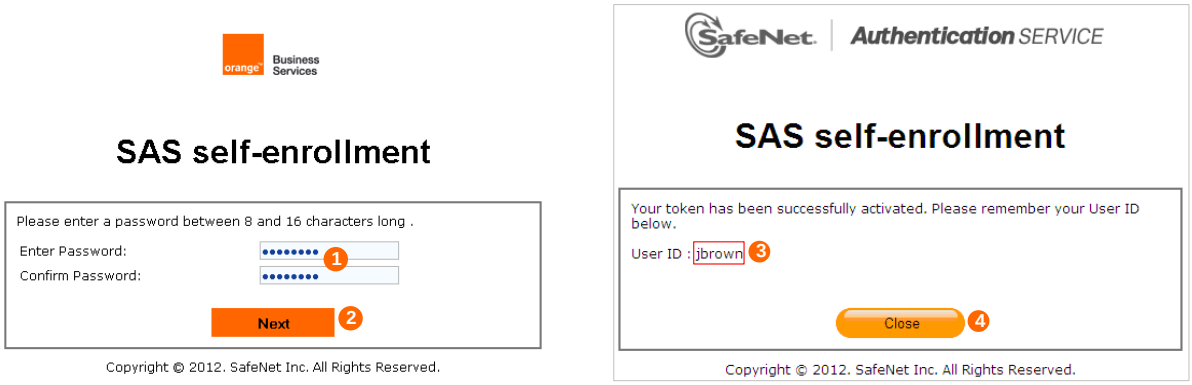

Figure 87: create password

- **"Complexity requirements not met" error message:** try to enter your password again making sure to meet complexity requirements.
- **"You have failed to provide the correct response too many times" error message:** contact your usual help desk.

how do I authenticate with my password?

You have the ability to test authentication with your password thanks to the SAS self-service portal.

1. **Within your e-mail client:** open the “SAS Self-enrollment” message 1 again, and click on the SAS self-service portal URL link 2: your web browser will connect to the self-service web site.

2. **Within the SAS self-service portal:** within the “Home” page click on “Sign In” 3, within the “Authenticate” page click on “Sign in using your token” 4.

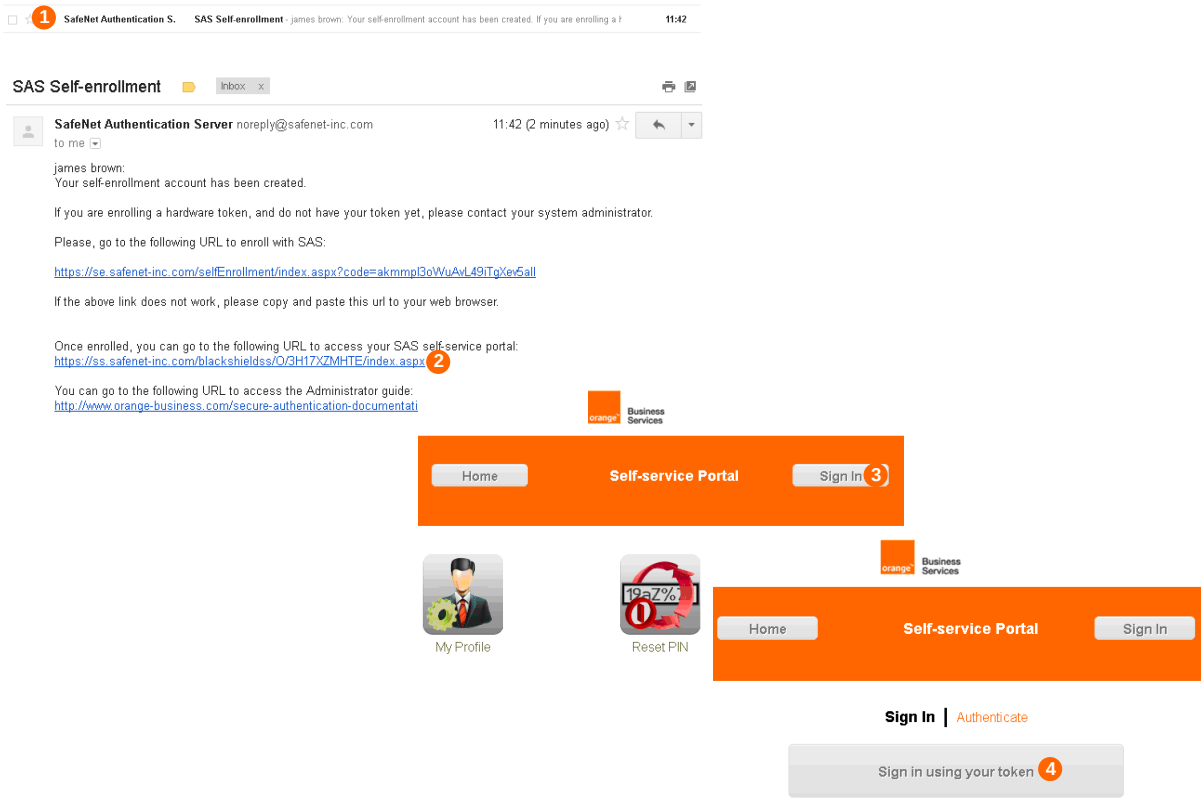

Figure 88: access to the SAS self-service portal sign in page

3. **Within the SAS self-service portal:** within the "Authenticate to Process" page enter your user ID in the "User ID" field ❶ and your password in the "OTP" field ❷, click on "OK" ❸. The "Sign Out" button ❹ displayed within the "Home" page indicates your authentication is successful.

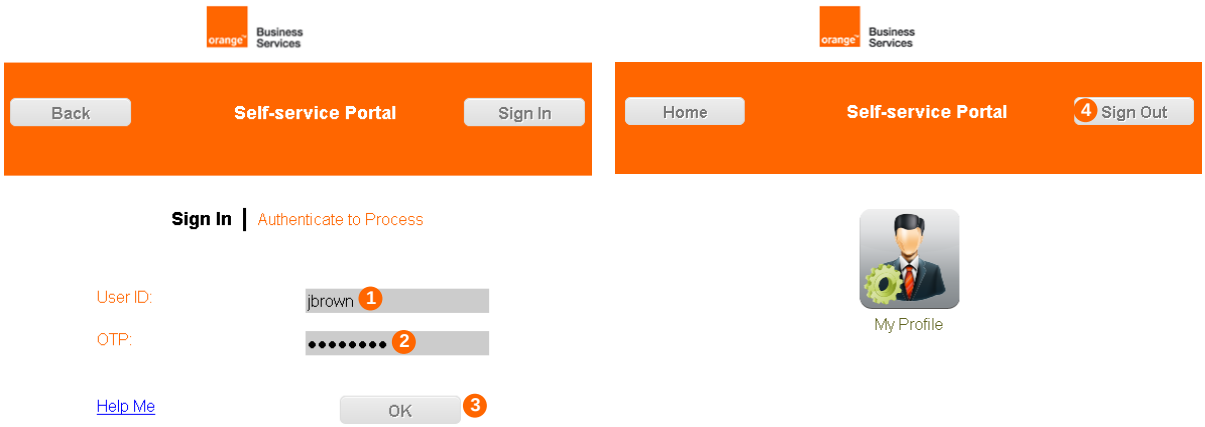

Figure 89: authenticate with password

- **"Your login attempt was not successful" error message:** click on "Home" and try to authenticate again, making sure to enter the correct password in the "OTP" field.

what to do if I forget my password?

resend my password by e-mail

1. **Within the SAS self-service portal:** within the "Home" page click on "Sign In" 1, within the "Authenticate" page click on "Send Sign in password by e-mail" 2, within the "Send Password by E-mail" page enter you user ID in the "User ID" field 3 and click on "Send" 4.

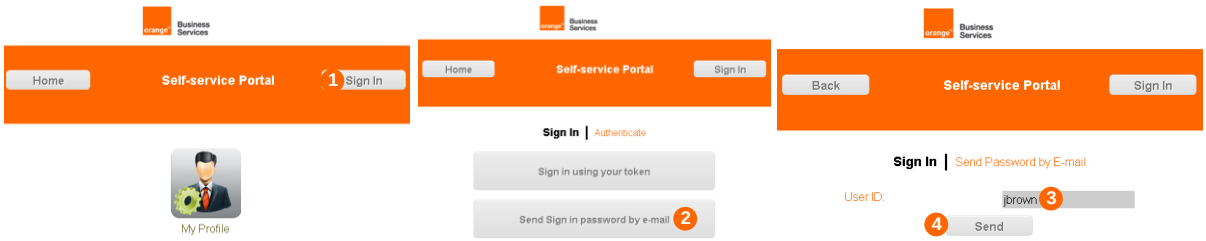

Figure 90: resend password by e-mail (1/2)

2. **Within your e-mail client:** open the "SAS Self-service Temporary Sign in Password" message 1, and click on the SAS self-service portal URL link: your web browser will connect to the self-service web site.

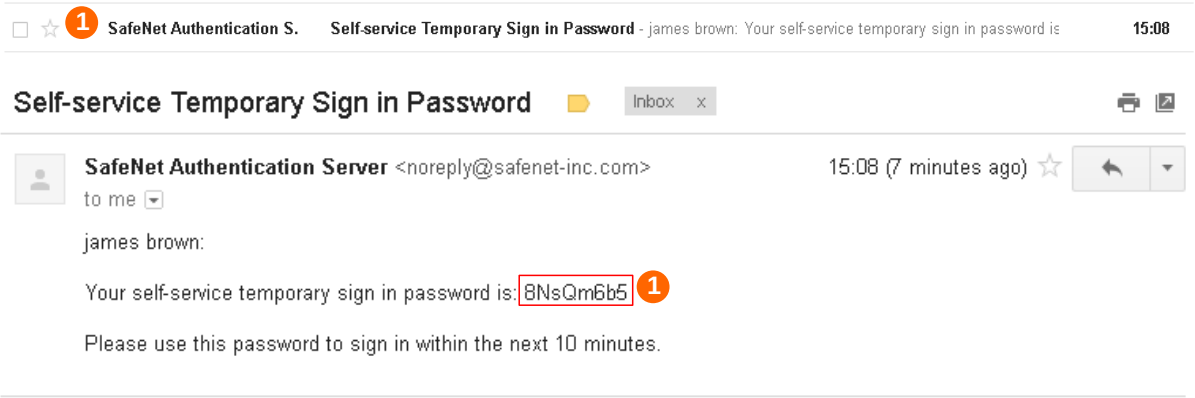

Figure 91: resend password by e-mail (2/2)

As mentioned within the e-mail, **you have to use this password to sign in within the next 10 minutes.**

- **"Self-service Temporary Sign in Password" e-mail not received:** verify if the mail is not stored in the "junk" folder of your e-mail client.

how do I change my password?

You have not the ability to change your password yourself: you have to use the "Send sign in password by e-mail" option from your SAS self-service portal instead.